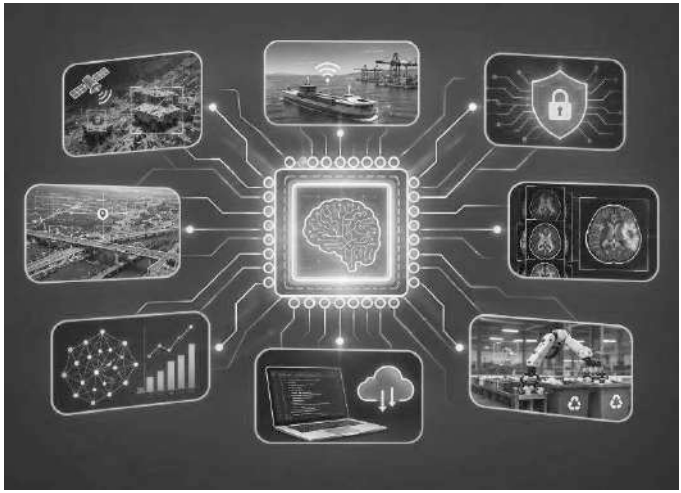
Національний університет «Одеська політехніка»



ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ТА ЦИФРОВІ ТЕХНОЛОГІЇ

МОНОГРАФІЯ

1256 1233 1996 LIHA-PRES
Львів-Торунь
Liha-Pres
2026

УДК 004:37:001:62
Р64

Авторський колектив:

Антощук С., Арсірій В., Арсірій О., Арсірій О., Бєлінський А., Бєляєв К., Бойко Н., Бондар Є., Вичужанін А., Вичужанін В., Винокурова О., Вовк О., Водка О., Гільгурт С., Гнатушенко В., Дейнеко Ж., Жихарієв В., Засідько А., Зеленський С., Зленський А., Іванов О., Каштан В., Ків А., Козловська Д., Козловський В., Котик Б., Ковальчук Л., Крантовський І., Кравченко О., Кунуп Т., Кутвицький М., Литвиненко С., Марченко С., Мендєлєва М., Міхалев К., Місюра С., Науменко С., Неласа Г., Нетребін Ю., Ніколенко А., Олійник В., Пелешко Д., Пелешко М., Пелешко С.-Д., Петров І., Положаєнко С., Прокофєєв А., Прокофєєва Л., Розломій І., Рудніченко М., Савельєв А., Саваневич В., Соловйов В., Тертус Ю., Табакова І., Трунова Т., Тужиков А., Філін Д., Фомін О., Хламов С., Хорошевська І., Шаповалова М., Шведов Д., Шибаєва Н., Шумейко К., Ярмілко А.

Рекомендовано до друку вченою порадою
Національного університету «Одеська політехніка»
(протокол №2 від 29.09.2026 р.)

Рецензенти:

Професор **С. Овермайер**, Університет Південного Нью-Гемпширу (США);
Професор **A. Kupin,** Криворізький національний університет (Україна)

Р64 **Інтелектуальні** системи та цифрові технології : монографія / під наук. ред. проф. В.Вичужаніна. – Львів-Торунь : Liha-Pres, 2026 – 338 с. Укр., англ. мовами.
ISBN 978-966-397-663-1
DOI https://doi.org/10.36059/978-966-397-663-1

У монографії відображені результати наукових досліджень у галузі інтелектуальних систем і технологій, заснованих на даних, управління та робототехніки, цифрових платформ і безпеки, моделювання, програмної інженерії та прикладних інформаційно-комунікаційних технологій. Матеріали монографії будуть корисними для аспірантів, магістрантів, науковців, викладачів закладів вищої освіти, інженерів та фахівців, які спеціалізуються у галузі інформаційних технологій та сучасних цифрових технологій.

УДК 004:37:001:62

ISBN 978-966-397-663-1

© Національний університет "Одеська політехніка", 2026
© Колектив авторів, 2026

CONTENTS

Preface……..…….5

Section 1 Intelligent systems and data-driven technologies

COMPARATIVE EVALUATION OF YOLO ARCHITECTURES FOR MILITARY VEHICLE RECOGNITION IN AEROSPACE IMAGERY
Ph.D., Kashtan V., Dr.Sci., Hnatushenko V.
Dnipro University of Technology, Ukraine………...*6*

CYBER-PHYSICAL COORDINATION OF AUTONOMOUS SHIPS AND SMART PORTS: A DISTRIBUTED SYSTEM-OF-SYSTEMS APPROACH
Dr.Sci., Vychuzhanin V., Ph.D., Vychuzhanin A.
Odessa Polytechnic National University, Ukraine………..*23*

A VIDEO STREAM ENCRYPTION ALGORITHMTHAT DOES NOT PROPAGATE ERRORS
Dr.Sci., Kovalchuk L., Dr.Sci., Hilgurt S., Ph.D., Nelasa H.
G.E. Pukhov Institute for Modelling in Energy Engineering of the NAS of Ukraine, Ukraine………...*54*

CONDITIONAL GENERATIVE MODELS WITH SYNTHETIC DATA QUALITY CONTROL FOR RECOGNITION OF UNDERREPRESENTED CATEGORIES OF MEDICAL IMAGES
Mikhalev K., Ph.D., Nikolenko A.
Odessa Polytechnic National University, Ukraine……*68*

COMPARATIVE ANALYSIS OF VLM FOR INFRASTRUCTURE DAMAGE CLASSIFICATION: A CASE STUDY OF UKRAINE
Ph.D., Ivanov O.[1], Bieliaiev K. [2], Oliinyk V. [3], Arsiriy O.[4]
[1,2,3]Odessa Polytechnic National University, Ukraine,
[4]Odesa State Maritime University, Ukraine……*82*

INTELLIGENT RISK-ORIENTED MULTIMODAL DATA ANALYSIS FOR ADAPTIVE RESOURCE CONTROL IN DECENTRALIZED NETWORKS
Ph.D., Rudnichenko M.[1], Ph.D., Shibaeva N.[1], Shumeiko K.[1], Shvedov D.[1], Kiporuk V.[1], Dr.Sci.,Petrov I.[2]
[1]Odessa Polytechnic National University, Ukraine,
[2]National University "Odessa Maritime Academy", Ukraine………*102*

INTELLIGENT SYSTEM FOR PLANT DISEASE IDENTIFICATION FROM IMAGES BASED ON DEEP LEARNING
Dr.Sci., Antoshchuk S., Ph.D., Kunup T., Kravchenko O.
Odessa Polytechnic National University, Ukraine………*127*

ACCURACY LIMITS OF MACHINE-LEARNING MODELS FOR DEFECTS AND DOPING IN GRAPHENE QUANTUM DOTS ACCURACY LIMITS OF MACHINE-LEARNING POTENTIALS FOR DEFECTS AND DOPING OF GRAPHENE QUANTUM DOTS
Tuzhikov A.[1], Dr.Sci., Solovyov V.[1,3], Dr.Sci., Kiv A.[2], Belinsky A.[4]
[1]State Institution 'K. D. Ushynsky South Ukrainian National Pedagogical University', Ukraine,
[2]Ben-Gurion University of the Negev, Israel,
[3]Vadym Hetman Kyiv National Economic University, Ukraine,
[4]State University of Economics and Technology, Ukraine……*151*

INTELLIGENT ANALYSIS OF HETEROGENEOUS DATA IN PROACTIVE ENERGY MANAGEMENT SYSTEMS OF SMART OBJECTS
Dr.Sci., Арсірій О.[1], Dr.Sci., Арсірій В.[2], Засідько А.[1], Крантовський І.[1]
[1] Odessa Polytechnic National University, Ukraine,
[2] Odessa State Academy of Civil Engineering and Architecture, Ukraine……*168*

Section 2 Control, robotics, and distributed systems

MODELS OF HYBRID HUMAN-MACHINE CONTROL FOR ROBOTIC SYSTEMS
Ph.D., Yarmilko A., Marchenko S.
Bohdan Khmelnytsky National University of Cherkasy, Ukraine……***183***

Section 3 Digital platforms, security, and ICT infrastructure

3D COMPUTER VISION SYSTEM FOR AUTOMATED WASTE GRASPING AND SORTING BY MOBILE ROBOTS
Ph.D., Boyko N.
Lviv Polytechnic National University, Ukraine,
Lviv National Stepan Gzhytsky University of Veterinary Medicine and Biotechnology, Ukraine……***202***

METHOD FOR INTEGRITY CONTROL OF DIGITAL TWIN DATA STREAMS BASED ON CRYPTOGRAPHIC CHAINING OF CONSECUTIVE MESSAGES
Ph.D., Rozlomii I.[1], Ph.D., Naumenko S.[2]
[1]Cherkasy State Technological University, Ukraine,
[2]Bohdan Khmelnytsky National University of Cherkasy, Ukraine……***222***

Section 4 Modeling, software engineering, and applied ICT

A METHOD FOR VERIFYING THE ACCURACY OF COMPUTATIONAL IMPLEMENTATIONS FOR SOLVING DYNAMIC SYSTEM MODELING PROBLEMS
Dr.Sci., Polozhaenko S., Dr.Sci., Fomin O., Prokofieva L., Ph.D., Prokofiev A., Ph.D. Savieliev A., Filin D.
Odessa Polytechnic National University, Ukraine……***235***

METHODOLOGICAL FRAMEWORK FOR PERFORMANCE TESTING AND EVALUATION OF RESTFUL API USING AUTOMATED TESTING TOOLS
Ph.D. Khlamov S., Mendielieva M., Ph.D. Vovk O., Trunova T., Ph.D. Deineko Zh., Lytvynenko S.
Kharkiv National University of Radio Electronics, Ukraine……***250***

MULTISTAGE SHORT-WAVE INFRARED IMAGE PROCESSING PIPELINE
Bondar Y.[1], Kutvytskyi M.[1],
Netrebin Y.[1], Dr. Sci., Savanevych V.[1], Ph.D., Khlamov S.[1], Dr.Sci., Zelensky S.[2], Ph.D., Khoroshevska I.[3], Ph.D., Tabakova I.[1]
[1] Kharkiv National University of Radio Electronics, Ukraine,
[2] Taras Shevchenko National University of Kyiv, Ukraine,
[3] Simon Kuznets Kharkiv National University of Economics, Ukraine……***267***

VOXEL-BASED MODELING OF THE EFFECT OF NON-UNIFORM FIBER DISTRIBUTION ON THE ELASTIC PROPERTIES OF FIBER-REINFORCED COMPOSITES
Ph.D., Vodka O., Ph.D. Shapovalova M., Ph.D. Misiura S., Zhykhariev V.
National Technical University "Kharkiv Polytechnic Institute", Ukraine……***284***

LORAWAN IN AVIATION: A COMPREHENSIVE ANALYSIS OF CYBER THREATS AND RESILIENCE STRATEGIES
Tertus Y., Kozlovska D., Dr.Sci., Kozlovsky V., Kotyk B.
State University "Kyiv Aviation Institute", Ukraine……***301***

FINE-TUNING SPECIFICS OF AUDIO-MODALITY LARGE LANGUAGE MODELS: OMNIVOICE, FISHAUDIO2(FISHSPEECH S2) AND QWEN3 AUDIO
Dr.Sci., Peleshko D.[1], Peleshko S.-D.[2], Dr.Sci., Vynokurova O.[3], Ph.D., Peleshko M.[4]
[1,3]Ivan Franko National University of Lviv, Ukraine
[2]Ukrainian Catholic University, Ukraine
[4]Lviv State University of Life Safety, Ukraine……***317***

PREFACE

The present monograph compiles materials derived from research papers presented at The International Scientific and Practical Workshop “Advanced Digital Technologies: Intelligent Systems, Modeling, and Data-Driven Control” (ADT-ISMDDC-2026), co-located with the XIV International Scientific and Practical Conference “Information Control Systems and Technologies – ICST-ODESA-2026.”

This collective volume reflects the outcomes of scientific investigations in the domains of intelligent systems and data-driven technologies, control and robotics, digital platforms and security, modeling, software engineering, and applied information and communication technologies. The monograph is organized in the form of research article-based chapters, grouped according to thematic sections that comprehensively represent the scope of studies conducted in the following areas: Intelligent Systems and Data-Driven Technologies; Control, Robotics, and Distributed Systems; Digital Platforms, Security, and ICT Infrastructure; and Modeling, Software Engineering, and Applied ICT.

Special emphasis is placed on addressing issues such as: Intelligent image and video analysis, machine learning and multimodal data processing, synthetic data generation, cyber-physical systems, autonomous platforms, and data-driven control and decision-making.

Considerable attention is also devoted to: robotic systems and computer vision, digital twin data integrity, information and video security, computational and physical modeling, automated software testing, image-processing technologies, ICT infrastructure resilience, and advanced audio-modality language models.

The results presented provide readers with valuable insights into contemporary approaches to the development and application of advanced digital technologies for solving complex scientific and engineering problems.

All articles included in this monograph correspond to the versions submitted by the authors. Full responsibility for the content of individual contributions rests solely with their respective authors.

The materials of the monograph will serve as a useful resource for postgraduate and master’s students, researchers, academic faculty, engineers, and specialists engaged in research and education in the fields of information technologies and advanced digital technologies.

The preparation of this collective work involved the contribution of scholars, including 16 Doctors of Science, 24 Candidates of Science, and 26 Ph.D. applicants.

Section 1 Intelligent systems and data-driven technologies

UDC 004.8:004.93
DOI

COMPARATIVE EVALUATION OF YOLO ARCHITECTURES FOR MILITARY VEHICLE RECOGNITION IN AEROSPACE IMAGERY

Ph.D., Kashtan V.[1][0000-0002-0395-5895], Dr.Sci., Hnatushenko V.[2][0000-0003-3140-3788]
Dnipro University of Technology, Ukraine
EMAIL: [1]vitalionkaa@gmail.com, [2]vvgnat@ukr.net

Abstract. *Recognition of military vehicles in aerospace imagery is a challenging computer vision task due to the small projected size of objects, complex background structure, partial occlusions, variability in spatial orientation, and the limited availability of representative annotated data. A particular challenge is the pronounced class imbalance, under which aggregate performance metrics may not fully characterize the recognition effectiveness for classes represented by a limited number of annotated instances. The aim of the study is to substantiate the selection of the most effective architecture among the investigated YOLO models for military-vehicle recognition in aerospace imagery based on a combination of overall and class-wise object-recognition performance metrics. The study was conducted using a formed own dataset comprising 2,274 aerospace images and 11,454 annotations belonging to four classes: military vehicles, tanks, trucks, and jeeps. The dataset was divided into 1,592 training images, 341 validation images, and 341 test images. All models used input images with a resolution of 640 × 640 pixels and were trained for 100 epochs. Based on the overall quantitative metrics, YOLOv8 demonstrated the most balanced performance, with Precision of approximately 0.65, Recall of 0.35, and mAP@50 of 0.30. The results showed that the investigated YOLO architectures differ in aggregate detection performance, while classes with a limited number of annotated instances consistently exhibit low Recall values. This indicates the substantial role of training-data representativeness in ensuring stable recognition performance across individual classes.*

Keywords: *aerospace imagery, military vehicle recognition, YOLO, deep learning, object detection, class imbalance, computer vision.*

1 Problem Statement

The rapid growth of aerospace observation data has increased the demand for automated methods capable of extracting semantically meaningful information from complex visual scenes. In security-oriented information systems, remote sensing and aerial imagery can support situational analysis, mapping, infrastructure monitoring, and object inventory tasks. Deep neural networks and machine-learning methods have become important components of this processing chain because they enable the extraction of spatial and semantic features directly from image data and can be adapted to large collections of remotely sensed imagery [1, 2, 3]. The applicability of such approaches has also been demonstrated in automated land-cover monitoring from optical satellite imagery [4]. The integration of imagery intelligence with open-source information further expands the diversity of available visual data, while simultaneously increasing heterogeneity in spatial resolution, illumination, image compression, viewing geometry, and scene composition [5].

Military-vehicle recognition in aerospace imagery represents a particularly difficult instance of the general object-detection problem [6]. A target may occupy

only a small fraction of an image, while surrounding terrain, roads, vegetation, buildings, shadows, and other vehicles generate strong background texture. The same object type can appear at different scales and orientations, and partial occlusion can remove the most discriminative visual features. These characteristics make the problem different from conventional close-range object detection, where targets are usually larger and acquisition conditions are more consistent. In addition, visually similar vehicle categories can be difficult to separate when the spatial resolution is insufficient to preserve fine structural details. A second challenge concerns the composition of training data. Military-domain imagery is usually less abundant and less balanced than generic computer-vision datasets. The cost of manual annotation is high because objects may be small, densely grouped, partly obscured, or visible only under difficult contrast conditions. If one generic category dominates the dataset, a detector can achieve seemingly acceptable aggregate performance while still performing poorly on rare fine-grained categories. For this reason, model-level metrics must be interpreted together with class-wise recall and error structure rather than as a single summary score. A third issue is methodological comparability. Reported recognition accuracy in the literature is often obtained on different image sources, different target taxonomies, different preprocessing pipelines, different model sizes, and different training budgets. Under such conditions, it is difficult to determine whether a performance gap is caused by the detector architecture or by differences in data and experimental configuration. The present work therefore treats controlled comparison itself as an important methodological requirement. Rather than searching for the individually optimized upper bound of every model, the study fixes the dataset partition, input resolution, and training budget so that the effect of architectural differences can be examined on a common basis. The scientific significance of the problem lies in understanding how the internal organization of single-stage detectors affects feature extraction and recognition under severe data imbalance. The practical significance lies in identifying a model that provides an acceptable balance between detection completeness and precision while also revealing the data-related limitations that cannot be solved by architectural changes alone. In this sense, the study considers intelligent analysis not merely as a ranking of detectors, but as a combined interpretation of aggregate metrics, class-wise behavior, confidence characteristics, and representative recognition errors.

2 Analysis of Previous Studies

The evolution of object detection has produced several major methodological families. Early approaches used handcrafted features and classical classifiers, while modern systems are dominated by convolutional neural networks, transformer-based models, and hybrid combinations of local and global feature processing. In aerial and military-oriented applications, these approaches differ not only in accuracy but also in computational complexity, robustness to scale variation, and sensitivity to limited training data. Region-based convolutional detectors introduced a two-stage logic in which candidate regions are first generated and then classified and refined. Mask R-CNN and related models demonstrated that region-based processing can provide strong localization and instance-level segmentation accuracy in remote-sensing imagery [7]. The main advantage of two-stage methods is their ability to devote substantial computation to candidate regions, but this advantage is accompanied by

higher latency and a more complex inference pipeline. For applications requiring rapid processing of many image tiles, the computational overhead of proposal generation and per-region processing can be restrictive. Single-stage detectors address this limitation by performing localization and classification directly from dense feature maps. The original YOLO formulation reframed object detection as a unified regression problem and established the real-time detection paradigm [8]. Subsequent YOLO generations progressively modified the backbone, feature-fusion neck, detection head, training losses, and feature aggregation strategy. The resulting family has become widely used in applied computer vision because it combines relatively simple deployment with strong speed-accuracy characteristics. Reviews of the YOLO family show that the main architectural trend has been toward more efficient feature reuse, stronger multi-scale fusion, and more flexible prediction heads [9]. Transformer-based detectors represent another important direction. DETR introduced an end-to-end set-prediction framework in which global attention replaces several hand-designed components of conventional detectors [10]. Transformer backbones and pyramid variants further improved long-range context modeling [11]. Their global receptive field is attractive for scenes in which contextual relationships are informative, but transformer-based models often require substantial computational resources and can be sensitive to training configuration. For high-resolution aerospace imagery containing many small targets, the challenge is to preserve fine local details while still exploiting broader contextual information. Recent work has also focused specifically on small-object and aerial detection. Guo et al. proposed enhanced interaction and cross-scale aggregation to improve the representation of small targets [12]. Zhao et al. combined YOLO and transformer components for infrared UAV vehicle detection, illustrating the potential of hybrid local-global feature extraction [13]. Other studies have investigated convolution-transform fusion for scale-invariant target detection in UAV imagery [14]. Semantic segmentation of spatial objects in aerial imagery has also been explored using hybrid neural-network approaches, including quantum-enhanced convolutional models for building extraction under complex background conditions [15]. Together, these works confirm that multi-scale representation is central to aerial object detection, but they also show that gains are usually coupled to dataset-specific design choices and training procedures. Within the authors' previous studies, comparative YOLO-based detection was investigated for aircraft in aerial imagery, including the influence of image preprocessing on false-negative reduction [16]. A separate study used a modified YOLO-OBB architecture for vehicle detection in aerial images, demonstrating the value of architecture customization when object orientation is important [17]. These studies provide useful methodological background, but their datasets, target classes, and model modifications differ from the present experiment; therefore, their numerical results cannot be directly transferred to the current task. Military-target recognition has also been studied using radar and low-altitude optical imagery. Deep-learning experiments on the MSTAR SAR dataset show high recognition accuracy under radar-specific acquisition conditions, while also highlighting the influence of speckle noise and aspect variation [18, 19]. In optical imagery, Kamran et al. emphasized the limitations of general-purpose datasets for low-altitude military-vehicle detection [20]. Hiippala demonstrated that open-source

and social-media imagery can support recognition of military vehicles, although uncontrolled imagery introduces substantial variability [21]. These studies confirm the domain-specific nature of the problem and the need for carefully interpreted results when image sources are heterogeneous. The literature therefore suggests three general conclusions (Tab.1).

Table 1

General comparison of modern object-detection approaches

Approach	Core principle	Main strengths	Limitations for aerospace imagery
Two-stage CNN detectors	Region proposals followed by classification/regression	Accurate localization; flexible region processing	Higher latency and more complex inference
Single-stage YOLO/SSD	Direct dense prediction from multi-scale features	Favorable speed-accuracy balance; simple deployment	Sensitivity to small targets and data distribution
Transformer detectors	Global attention and set prediction	Strong contextual modeling	Higher computational cost; training sensitivity
Hybrid CNN-transformer	Local convolution plus global attention/fusion	Combines local detail with contextual features	More complex architecture and optimization

First, no single detector family is universally superior across all acquisition conditions and target scales. Second, architectural innovation must be evaluated together with dataset composition because rare classes can dominate the error profile. Third, direct numerical comparison across studies is often inappropriate when target taxonomies, image sources, preprocessing, and training protocols differ. These observations motivate a controlled within-family analysis in which different YOLO generations are compared under the same verified experimental settings

3 Unresolved Issues

Despite substantial progress in object detection, four unresolved issues remain important for military-vehicle recognition in aerospace imagery. First, detector architectures are rarely compared under strictly identical experimental conditions. Reported gains may result not only from architectural changes but also from differences in dataset splits, augmentation, input size, training duration, or model-specific hyperparameter tuning. Without a common protocol, the independent contribution of architecture is difficult to isolate. Second, severe class imbalance complicates performance assessment. Aggregate or micro-averaged metrics may be dominated by the majority class, while a single mAP value can obscure poor class-wise AP or recall for rare categories. This problem is particularly relevant to the present dataset, in which the generic military-vehicle class accounts for 98.76% of retained annotations, whereas tank, truck, and jeep together represent only 1.24%. Third, it remains unclear whether architectural improvements in gradient flow, feature

reuse, or spatial attention can compensate for insufficient representative training data. A controlled comparison is therefore needed to determine whether minority-class errors are architecture-dependent or whether all models exhibit a similar detection-versus-background failure pattern. Finally, heterogeneous acquisition conditions introduce additional uncertainty. The author-created dataset combines publicly available aerial imagery rather than data from a single controlled sensor campaign, and complete metadata on platform, ground sampling distance, altitude, viewing geometry, and acquisition date are unavailable for every image. Accordingly, the study does not attribute performance to specific sensors or acquisition conditions; the absence of such stratified analysis is considered a limitation and a direction for future research.

4 Objective of the Article

The objective of the study is to substantiate the selection of the most effective architecture among YOLOv5, YOLOv8, YOLOv9, and YOLOv11 for military-vehicle recognition in aerospace imagery based on an integrated analysis of overall and class-wise detection performance. To achieve this objective, the following research tasks were formulated:

– to form and harmonize an author-created dataset of aerospace images using a unified taxonomy of military-vehicle classes;

– to analyze the distribution of annotated object instances and assess the degree of class imbalance in the formed dataset;

– to examine the principal structural characteristics of YOLOv5, YOLOv8, YOLOv9, and YOLOv11 that distinguish the investigated detection architectures;

– to ensure comparable conditions for training and evaluating the investigated architectures using identical data subsets, input image resolution, and training duration;

– to evaluate the investigated architectures using overall detection metrics, including Precision, Recall, F1-score, mAP@50, and mAP@50–95;

– to examine representative detection results in aerospace scenes and identify characteristic recognition errors;

– to substantiate the selection of the architecture that provides the most favorable combination of overall and class-wise detection characteristics for the investigated dataset;

– to identify the principal limitations of the conducted study and determine directions for further improvement of military-vehicle recognition in aerospace imagery.

5 Main Content

5.1 General analytical framework

The proposed analytical framework combines data preparation, controlled model training, multi-level evaluation, and interpretation of model errors. The workflow begins with a heterogeneous collection of aerospace images and proceeds through annotation harmonization, dataset partitioning, model training, quantitative evaluation, class-wise analysis, and comparative interpretation. The main design principle is experimental consistency: all four detector generations are evaluated on the same image subsets and with the same verified high-level settings. This

organization prevents the comparative conclusions from being dominated by differences in dataset partition or training duration.

The framework distinguishes three analytical levels. The first is the model level, represented by Precision, Recall, F1-score, mAP@50, and mAP@50-95. The second is the class level, where diagonal elements of normalized confusion matrices are interpreted as class-wise recall. The third is the scene level, where representative test images are used to examine incomplete detection, class substitution, duplicate predictions, and false positives. Combining these levels is essential because a single aggregate metric cannot explain why a detector succeeds or fails on underrepresented classes.

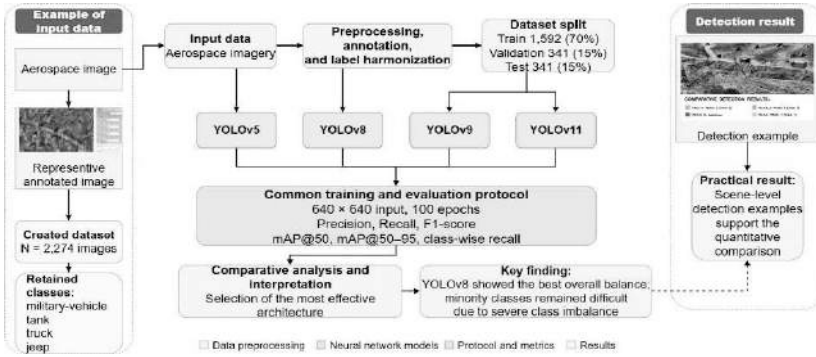


Figure 1. Controlled comparative framework with representative practical examples

5.2 Dataset formation, annotation, and harmonization

The experimental basis is an author-created custom dataset assembled from publicly accessible aerospace imagery and aerial-photography materials. The final collection contains 2,274 images. Because the data originate from heterogeneous sources rather than one controlled acquisition campaign, complete sensor metadata are not available uniformly. This limitation prevents a statistically rigorous sensor-by-sensor comparison, but the heterogeneous collection is useful for evaluating the behavior of the models on visually diverse scenes.

Object annotation was performed in the Computer Vision Annotation Tool (CVAT). Each retained target was assigned a class label and a bounding-box localization. The original annotation schema contained labels that were either outside the target problem or duplicated semantically. Three labels associated with non-vehicle content were excluded, while duplicate names for the generic military-vehicle category were merged. After harmonization, four target classes remained: military-vehicle, tank, truck, and jeep. This taxonomy was fixed before the data were divided into training, validation, and test subsets. The dataset was partitioned into 1,592 training images, 341 validation images, and 341 test images, corresponding approximately to a 70%/15%/15% split (Tab.2). The same image subsets were retained for all architectures. The training set was used for optimization, the validation set for model-level quantitative comparison, and the test subset for representative qualitative analysis. This distinction is important because it avoids mixing final-epoch validation metrics with scene-level test examples.

Table 2

Image-level dataset partition

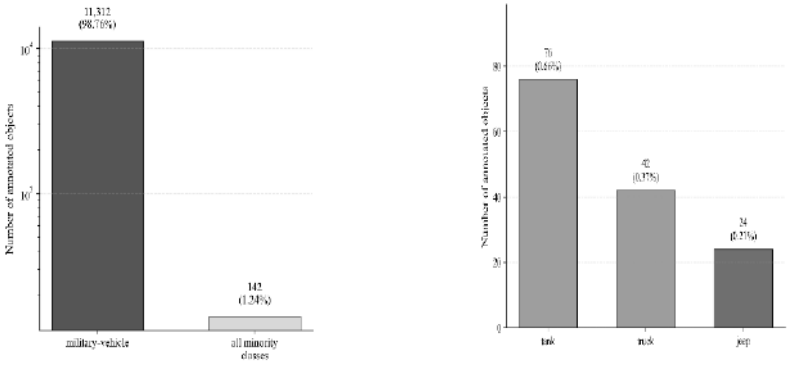
Subset	Number of images	Approximate share
Training	1,592	70%
Validation	341	15%
Test	341	15%
Total	2,274	100%

The harmonized annotation set contains 11,454 object instances. Its most important characteristic is extreme imbalance. As summarized in Table 3, the generic military-vehicle class strongly dominates the dataset, with 11,312 annotations (98.76%). In contrast, the fine-grained classes are represented by only 76 tank annotations (0.66%), 42 truck annotations (0.37%), and 24 jeep annotations (0.21%). Thus, the three minority classes together account for only 142 annotations, corresponding to 1.24% of the complete annotation set. The numerical distribution reported in Table 3 is visualized in Figure 2. Figure 2(a) compares the dominant military-vehicle class with all minority classes combined, clearly illustrating the scale of the imbalance: 11,312 annotations belong to the generic class, whereas only 142 annotations represent tank, truck, and jeep together. Figure 2(b) provides a detailed view of the minority classes and shows that tank is the most represented fine-grained category with 76 instances, followed by truck with 42 and jeep with 24 annotations. This two-level visualization makes it possible to demonstrate both the global class imbalance and the internal distribution of the underrepresented categories. The imbalance illustrated in Figure 2 has two important consequences for the interpretation of the experimental results. First, aggregate performance metrics are strongly influenced by the dominant military-vehicle class and therefore may overestimate the practical recognition capability for rare vehicle types. Second, the small number of minority-class examples makes class-wise recall sensitive to individual detections. For example, when only a few dozen truck or jeep instances are available, a single additional correct or incorrect prediction can noticeably affect normalized confusion-matrix values and the shape of precision–confidence curves.

Table 3

Distribution of object annotations by class

Class	Annotated objects, n	Share of all annotations
military-vehicle	11,312	98.76%
tank	76	0.66%
truck	42	0.37%
jeep	24	0.21%
Total	11,454	100%



a b

Figure 2. Distribution of annotated object instances in the harmonized dataset: a – comparison between the dominant military-vehicle class and the combined minority classes; b – detailed distribution of tank, truck, and jeep annotations

Consequently, the class distribution should be treated not merely as a descriptive characteristic of the dataset, but as one of the key factors explaining the differences between aggregate and class-specific recognition performance.

5.3 YOLO architecture fundamentals

All four compared models belong to the single-stage YOLO family (Fig.3). In a general form, a modern YOLO detector consists of three functional parts: a backbone, a neck, and a detection head. The backbone converts the input image into hierarchical feature maps. The neck combines features from different spatial scales so that high-level semantic information can be merged with finer localization cues. The head transforms the fused features into bounding-box and class predictions. This three-stage logic is common to several YOLO generations, but the internal modules and prediction mechanisms have changed substantially over time [9, 22].

Multi-scale feature processing is particularly important for aerospace imagery. Small objects require high-resolution feature maps because deep low-resolution layers can lose spatial detail. At the same time, reliable classification benefits from deeper semantic features with a larger receptive field. The neck therefore plays a central role by combining features from different levels. FPN-like top-down pathways transfer semantic information to higher-resolution maps, while PAN-like bottom-up pathways reinforce localization information. This general logic is present in YOLOv5, YOLOv8, and YOLOv11, although the block used at each fusion stage differs [22, 23]. The compared generations also illustrate the transition from anchor-based to anchor-free detection. Historical YOLOv5 uses predefined anchor boxes, whereas YOLOv8 and YOLOv11 use an anchor-free decoupled head in which box regression and class prediction are handled by separate branches [22, 23]. YOLOv9 differs conceptually because its main contribution is not only a new feature block but also an explicit strategy for preserving useful gradient information during learning [24]. These differences justify treating the selected models as distinct neural-network architectures rather than merely software versions.

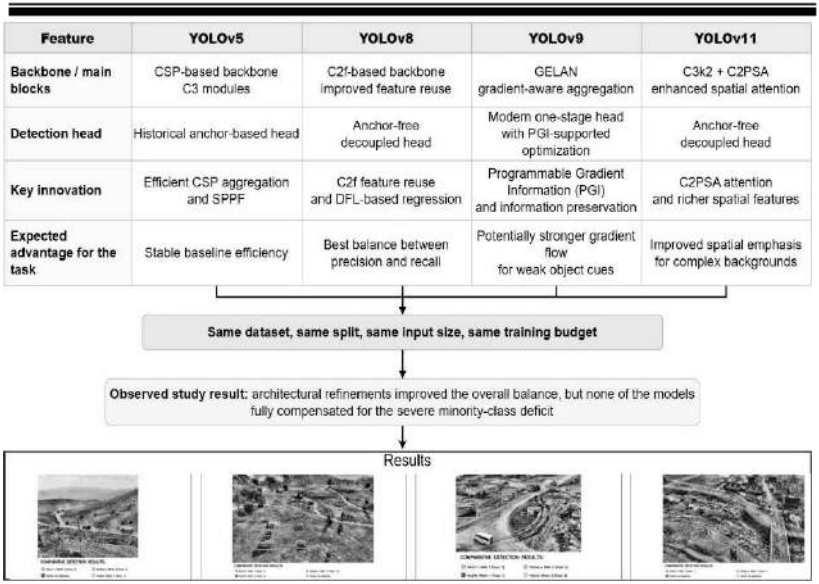


Figure 3. Comparative characteristics of the evaluated YOLO architectures and representative scene-level evidence

5.4 Comparative architectural interpretation

The architectural comparison shows that the four models differ at several levels simultaneously (Table 4). YOLOv5 represents the anchor-based CSP/SPPF design. YOLOv8 changes both internal feature reuse and the prediction head. YOLOv9 explicitly focuses on information preservation and gradient quality. YOLOv11 introduces a newer CSP-derived block together with position-sensitive attention [25]. These differences make the comparison informative even though all four models belong to one detector family.

Table 4

Comparative characteristics of the evaluated YOLO architectures

Feature	YOLOv5	YOLOv8	YOLOv9	YOLOv11
Principal feature block	C3 / CSP	C2f	GELAN-based aggregation	C3k2
Context/pooling	SPPF	SPPF	GELAN	SPPF + C2PSA
Detection concept	Anchor-based	Anchor-free	PGI-assisted	Anchor-free
Main emphasis	CSP efficiency	Feature reuse	Information preservation	Spatial attention
Small-object relevance	Multi-scale fusion	C2f + DFL	Gradient preservation	Attention + fusion

At the same time, the shared YOLO paradigm is methodologically useful. Because the models remain single-stage detectors with broadly comparable deployment logic, the experiment avoids the larger confounding that would arise from mixing fundamentally different two-stage, transformer, and hybrid pipelines. The study therefore does not claim that YOLO is universally superior; rather, it uses the family as a controlled architectural sequence through which the relation between feature design and recognition behavior can be analyzed.

5.5 Experimental protocol and evaluation criteria

All four models were trained using the same image partition. The verified high-level settings were a 640×640 pixel input resolution and a fixed 100-epoch training budget. The same training, validation, and test image subsets were used for all architectures. No systematic hyperparameter optimization or architecture-specific ablation study was performed. This choice means that the reported values should be interpreted as results under one controlled configuration rather than the maximum attainable performance of each detector. The quantitative comparison uses standard object-detection metrics. Precision characterizes the proportion of accepted detections that correspond to reference objects, while Recall measures the proportion of reference objects retrieved by the detector. F1-score summarizes their balance through the harmonic mean. Average Precision integrates the precision-recall relation for an individual class, and mean Average Precision averages class-level AP values. mAP@50 evaluates detection at an IoU threshold of 0.50, whereas mAP@50-95 summarizes performance across progressively stricter IoU thresholds.

The normalized confusion matrix is used for class-wise interpretation. The diagonal value for a class is treated as class-wise recall; therefore, a value of 0.11 for jeep means that approximately 11% of reference jeep instances were correctly detected and assigned to the jeep class under the evaluation settings. Such values are particularly informative in this dataset because the class distribution is extremely uneven.

5.6 Overall quantitative results

The overall quantitative performance of the four evaluated YOLO architectures was compared using Precision, Recall, F1-score, mAP@50, and mAP@50–95. These metrics characterize complementary aspects of detector performance, including the reliability of positive predictions, detection completeness, the balance between Precision and Recall, and localization accuracy at different Intersection over Union thresholds. The resulting validation metrics are summarized in Table 5.

Table 5

Overall validation performance of the compared architectures

Metric	YOLOv8	YOLOv11	YOLOv9	YOLOv5
Precision	≈0.65	≈0.65	≈0.45	≈0.52
Recall	≈0.35	≈0.28	≈0.28	≈0.20
mAP@50	≈0.30	≈0.28	0.29	0.23
mAP@50-95	≈0.14	≈0.13	≈0.15	≈0.14
F1-score (approx.)	≈0.46	≈0.39	≈0.35	≈0.29

As shown in Table 5, YOLOv8 provides the most favorable overall balance among the four evaluated architectures. It achieves a Precision of approximately 0.65, a Recall of approximately 0.35, and an mAP@50 of approximately 0.30. YOLOv11 reaches a similar Precision of approximately 0.65 but a lower Recall of approximately 0.28, indicating that its accepted detections are comparatively reliable, while a larger proportion of reference objects remains undetected. YOLOv9 achieves an mAP@50 of approximately 0.29, which is close to that of YOLOv8, but its Precision is lower, at approximately 0.45. YOLOv5 demonstrates the lowest Recall (approximately 0.20) and the lowest mAP@50 (approximately 0.23) under the reported fixed experimental configuration.

As shown in Table 5, YOLOv8 achieves the highest aggregate F1-score (0.46), offering the best precision-recall balance. However, given the severe dataset imbalance, overall metrics fail to accurately reflect individual vehicle category performance, strictly necessitating the subsequent class-wise analysis.

5.7 Class-wise recognition and imbalance effects

To determine whether the aggregate performance differences observed in Table 5 are preserved across individual vehicle categories, the normalized confusion matrices of the four architectures were analyzed at the class level. The diagonal elements of the normalized matrices were interpreted as class-wise Recall, i.e., the proportion of reference objects of a given class that were correctly detected and assigned to that class. The obtained values for military-vehicle, tank, truck, and jeep are summarized in Table 6.

Table 6

Class-wise recall derived from normalized confusion matrices

Class	YOLOv8	YOLOv11	YOLOv9	YOLOv5
military-vehicle	0.66	0.58	0.62	0.71
tank	0.17	0.17	0.17	0.22
jeep	0.11	0.11	0.11	0.00
truck	0.14	0.11	0.40	0.00

To provide a more intuitive comparison of the class-specific behavior of the four architectures, the Recall values from Table 6 are additionally visualized as a heat map in Figure 4. The visualization highlights both the substantially higher Recall of the dominant military-vehicle class and the consistently lower values obtained for the three fine-grained minority classes. As demonstrated by Table 6 and Figure 4, the class-wise results reveal a pattern that is not evident from the aggregate performance metrics. Recall for the generic military-vehicle class ranges from 0.58 to 0.71 across the four architectures, whereas the three fine-grained classes are recognized much less completely. Tank Recall remains within a narrow range of 0.17–0.22. Jeep Recall reaches only 0.11 for YOLOv8, YOLOv11, and YOLOv9, and decreases to 0.00 for YOLOv5. Truck Recall shows greater variation, ranging from 0.00 for YOLOv5 to 0.40 for YOLOv9. This contrast between the dominant and minority classes is clearly visible in Figure 4 and indicates that the principal source of error is incomplete

detection of underrepresented objects rather than uniformly poor recognition across all categories.

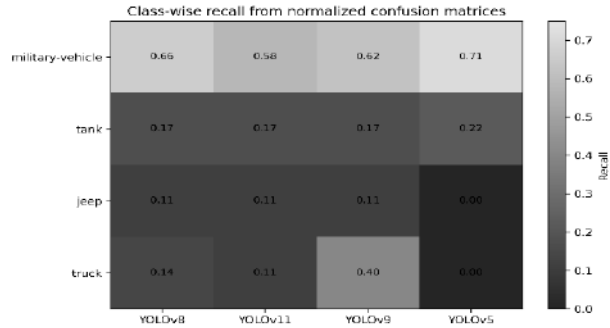


Figure 4. Class-wise recall across the four detector architectures

Even YOLOv8, which provides the best overall balance according to Table 5, retrieves only a limited proportion of tank, truck, and jeep instances. Its aggregate advantage is therefore driven primarily by stronger performance on the well-represented generic military-vehicle class. The consistency of low minority-class Recall across structurally different architectures is analytically important. YOLOv5, YOLOv8, YOLOv9, and YOLOv11 differ in anchor logic, feature reuse, gradient-flow organization, and spatial-attention mechanisms; nevertheless, all four models experience substantial difficulty when only a limited number of annotated training examples are available. This cross-model pattern supports the interpretation that the recognition ceiling for the minority classes is primarily data-limited rather than solely architecture-limited. Architectural design remains important for overall detector performance, but it cannot fully compensate for insufficient quantity and diversity of representative training examples.

5.8 Scene-level qualitative analysis

Representative test scenes, summarized visually in Figure 5, were used to complement the validation metrics with interpretable examples. In the forested scene (Fig.5a), five reference targets were treated as truck-class objects. YOLOv8 produced three truck detections, YOLOv11 produced two, YOLOv5 one, and YOLOv9 none. This example illustrates the combined effect of small target size, background texture, and partial occlusion. In the open-grassland scene (Fig.5b), the reference annotation contains six tanks. YOLOv8 produced eleven tank-labeled predictions and YOLOv11 seven, meaning that the number of predictions exceeded the number of reference objects and some outputs necessarily corresponded to duplicate or false-positive detections. YOLOv9 produced two truck-labeled predictions and YOLOv5 produced none. The example shows why raw detection counts must not be interpreted as the number of correctly recognized unique objects.

In the unpaved-road scene (Fig.5c), the reference contains five tank targets and a visible civilian minibus that is not part of the target set. YOLOv11 produced seven tank-labeled predictions and YOLOv8 five. YOLOv9 produced one truck-labeled

prediction, while YOLOv5 produced three truck-labeled predictions and incorrectly labeled the minibus as a truck. This false positive illustrates a failure mode that can be operationally important even when aggregate precision is acceptable. The fourth representative scene (Fig.5d) contains one low-salience tank target. YOLOv8 and YOLOv11 detect the object, whereas YOLOv9 and YOLOv5 produce no detection. Taken together, these examples do not replace dataset-level evaluation, but they help explain why model ranking should consider both numerical metrics and scene-specific failure patterns.

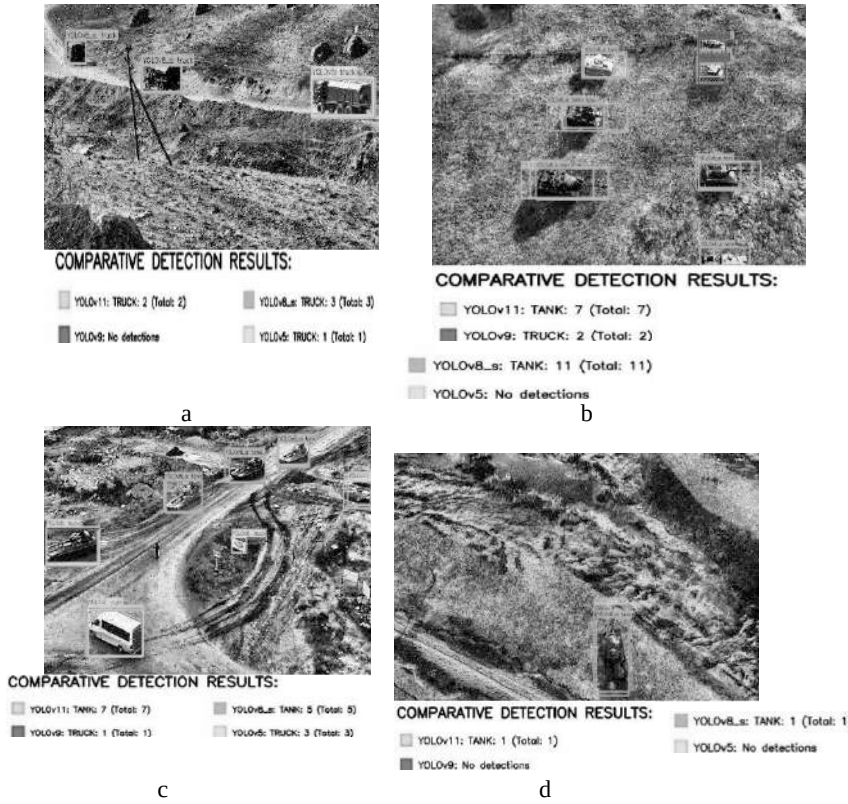


Figure 5. Representative scene-level detection results for the four test scenes: a – forecasted area; b – open grassland; c – unpaved road; d – riverside settlement

5.9 Discussion of scientific results

The results confirm that architectural changes within the YOLO family influence the balance among precision, recall, and localization quality. YOLOv8 provides the strongest overall balance in the reported experiment. YOLOv11 achieves similar precision but retrieves fewer objects, while YOLOv9 achieves a competitive

mAP@50 but lower precision. YOLOv5 remains useful as an efficient baseline but shows the weakest recall under the fixed protocol. A comparison with earlier aerospace-detection studies must be made cautiously. The authors' preprocessing-enhanced aircraft study reported a substantial reduction in false negatives, while the modified YOLOv11-OBB work achieved much higher absolute metrics on a different high-resolution vehicle dataset [13,14]. Those values cannot be directly compared with the present results because the target classes, source imagery, annotation rules, model modifications, and training procedures are different. The current experiment is intentionally more constrained: it uses one imbalanced author-created dataset and compares unmodified selected YOLO generations under a common high-level protocol. The class-wise analysis provides the central scientific interpretation. If architecture were the dominant limitation, one would expect the newer models to remove most of the minority-class deficit. Instead, tank and jeep recall remain low across all four architectures, while truck recall changes but remains unstable. The similarity of the failure pattern across structurally different models indicates that data quantity and diversity are at least as important as the architectural choice. This conclusion is consistent with earlier work emphasizing the limitations of generic or insufficiently specialized datasets for military aerial recognition [17]. The results also demonstrate the importance of separating recognition completeness from confidence. A model can maintain comparatively high precision while missing many objects. Conversely, increasing the number of predictions can improve recall but also generate duplicates or false positives. For this reason, the most suitable architecture depends on the practical objective. In a task where missed objects are particularly undesirable, YOLOv8's higher recall makes it preferable among the tested models. In a task where false positives are more costly, threshold tuning and additional class-specific validation may be required. The study has several limitations. First, the dataset is strongly imbalanced. Second, complete sensor metadata are not available for every image, preventing acquisition-condition stratification. Third, no formal inter-annotator agreement experiment was performed. Fourth, the training budget was fixed and systematic hyperparameter optimization was outside the experimental scope. Finally, the results apply only to the selected four architectures and should not be interpreted as an exhaustive benchmark of all object-detection paradigms.

6 Conclusions

The study developed an intelligent comparative analysis of military-vehicle recognition accuracy in aerospace imagery using four architecturally distinct YOLO generations. The analysis was based on an author-created dataset of 2,274 images and 11,454 retained object annotations. A common data partition, 640×640 input resolution, and fixed 100-epoch training budget were used to reduce configuration-related confounding. The architectural analysis showed that the compared models represent different design stages within the YOLO family. YOLOv5 uses a CSP/C3 backbone, SPPF, and the historical anchor-based detection logic. YOLOv8 introduces C2f feature reuse, an anchor-free decoupled head, and distribution-based box regression. YOLOv9 focuses on information preservation through GELAN and Programmable Gradient Information. YOLOv11 develops the YOLOv8-style design further by introducing C3k2 and C2PSA spatial attention while retaining anchor-free multi-scale detection. Under the reported fixed configuration, YOLOv8 achieved the

most favorable overall balance, with Precision of approximately 0.65, Recall of approximately 0.35, and mAP@50 of approximately 0.30. YOLOv11 achieved similar precision but lower recall. YOLOv9 reached a comparable mAP@50 but lower precision, whereas YOLOv5 showed the lowest recall and mAP@50 among the evaluated models. The most important result is the strong divergence between aggregate and class-wise performance. While the generic military-vehicle class reaches recall values between 0.58 and 0.71, the fine-grained tank, truck, and jeep classes remain substantially lower. Because these classes together represent only 1.24% of the annotations, the recurring detection-versus-background errors across all four architectures indicate a data-limited recognition ceiling. Architectural improvements change the error profile but do not compensate for the lack of representative examples. Future research should therefore prioritize expansion and rebalancing of the minority classes, including additional geographic, seasonal, viewing-angle, and background diversity. A second direction is stratified evaluation by acquisition conditions once reliable metadata are available. A third direction is a controlled sensitivity analysis of input resolution, training duration, augmentation, and other hyperparameters. Finally, subsequent studies should extend the comparison to newer YOLO generations and hybrid CNN-transformer detectors while preserving the same dataset partition and evaluation protocol. Such an extension would make it possible to distinguish genuine architectural progress from gains caused by different experimental settings.

Acknowledgements. This research is carried out as part of the scientific project no.0126U000995 “Intelligent technologies for analyzing spatiotemporal changes in aerospace imagery to support decision-making under conditions of armed aggression,” funded by the Ministry of Education and Science of Ukraine at the expense of the state budget.

Declaration on generative AI. The authors used Grammarly to check the grammar and spelling. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication’s content.

References

[1] Peng, H., Zhang, Y., Yang, S., & Song, B. (2019). Battlefield image situational awareness application based on deep learning. IEEE Intelligent Systems, 35, 36-43. https://doi.org/10.1109/MIS.2019.2942701

[2] Mei, C., Fan, Z., Zhu, Q., Yang, P., Hou, Z., & Jin, H. (2023). A novel scene matching navigation system for UAVs based on vision/inertial fusion. IEEE Sensors Journal, 23, 6192-6203. https://doi.org/10.1109/JSEN.2023.3242045

[3] Zhou, L., Leng, S., Liu, Q., & Wang, Q. (2021). Intelligent UAV swarm cooperation for multiple targets tracking. IEEE Internet of Things Journal, 9, 743-754. https://doi.org/10.1109/JIOT.2021.3106339

[4] Kashtan, V. Yu., & Hnatushenko, V. V. (2025). Intelligent technology for land cover monitoring due to amber mining on optical satellite images. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, (3), 156–164. https://doi.org/10.33271/nvngu/2025-3/156

[5] Scuro, V. (2025). Open-source intelligence (OSINT) for researchers and practitioners. Springer. https://doi.org/10.1007/978-3-032-02014-7_2

[6] Sumari, A. D. W., et al. (2022). Automatic target recognition and identification for military ground-to-air observation tasks using support vector machine and information fusion. In Proceedings of the International Conference on ICT for Smart Society (ICISS) (pp. 1-8). IEEE. https://doi.org/10.1109/ ICISS55894.2022.9915201

[7] Su, H., et al. (2019). Object detection and instance segmentation in remote sensing imagery based on precise Mask R-CNN. In IGARSS 2019 - IEEE International Geoscience and Remote Sensing Symposium (pp. 1454-1457). IEEE. https://doi.org/10.1109/ IGARSS.2019.8898160

[8] Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 779-788). https://doi.org/10.1109/CVPR.2016.91

[9] Terven, J., Córdova-Esparza, D.-M., & Romero-González, J.-A. (2023). A comprehensive review of YOLO architectures in computer vision: From YOLOv1 to YOLOv8 and YOLO-NAS. Machine Learning and Knowledge Extraction, 5(4), 1680-1716. https://doi.org/10.3390/make5040083

[10] Carion, N., Massa, F., Synnaeve, G., Usunier, N., Kirillov, A., & Zagoruyko, S. (2020). End-to-end object detection with transformers. In A. Vedaldi, H. Bischof, T. Brox, & J.-M. Frahm (Eds.), Computer Vision - ECCV 2020 (pp. 213-229). Springer. https://doi.org/10.1007/978-3-030-58452-8_13

[11] Wang, W., Xie, E., Li, X., et al. (2021). Pyramid vision transformer: A versatile backbone for dense prediction without convolutions. In Proceedings of the IEEE/CVF International Conference on Computer Vision (pp. 568-578). https://doi.org/10.1109/ICCV48922.2021.00061

[12] Guo, Z., Mu, X., Chang, C., et al. (2025). An enhanced framework for small object detection with middle-order interaction and adaptive cross-scale aggregation. Engineering Applications of Artificial Intelligence, 130, 107736. https://doi.org/10.1016/j.engappai.2024.107736

[13] Zhao, X., Xia, Y., Zhang, W., Zheng, C., & Zhang, Z. (2023). YOLO-ViT-based method for unmanned aerial vehicle infrared vehicle target detection. Remote Sensing, 15, 3778. https://doi.org/10.3390/rs15153778

[14] Alrayes, F. S., Ahmad, N., Alshuhail, A., et al. (2025). Convolutional transform learning-based fusion for scale-invariant long-term target detection in UAVs. Scientific Reports, 15. https://doi.org/10.1038/s41598-024-51123-x

[15] Kashtan, V., Hnatushenko, V., Babets, D., Cyran, K., & Wereszczyński, K. (2025). Hybrid quantum CNN-based information technology for building semantic segmentation in aerial imagery. PhD Workshop on Artificial Intelligence in Computer Science at CoLInS-2025, 150–162. https://ceur-ws.org/Vol-4015/paper11.pdf

[16] Kashtan, V., Radionov, Y., & Hnatushenko, V. (2025). Aircraft detection in aerial imagery based on YOLO architectures. CEUR Workshop Proceedings, 3983, 196-208. https://ceur-ws.org/Vol-3983/paper15.pdf

[17] Hnatushenko, V., Kashtan, V., & Kazymyrenko, O. (2025). Information technology for detecting cars on aerial imaging using a modified YOLO-OBB architecture. CEUR Workshop Proceedings, 4005, 293-304. https://ceur-ws.org/Vol-4005/paper20.pdf

[18] Geng, Z., Xu, Y., Wang, B.-N., Yu, X., Zhu, D.-Y., & Zhang, G. (2023). Target recognition in SAR images by deep learning with training data augmentation. Sensors, 23, 941. https://doi.org/10.3390/s23020941

[19] Jacob, S., Wall, J., & Sharif, S. (2023). Analysis of deep neural networks for military target classification using synthetic aperture radar images. In Proceedings of 3ICT 2023 (pp. 227-233). IEEE. https://doi.org/10.1109/3ICT60104.2023.10391600

[20] Kamran, F., Shahzad, M., & Shafait, F. (2018). Automated military vehicle detection from low-altitude aerial images. In 2018 Digital Image Computing: Techniques and Applications (DICTA) (pp. 1-8). IEEE. https://doi.org/10.1109/DICTA.2018.8615865

[21] Hiippala, T. (2017). Recognizing military vehicles in social media images using deep learning. In 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE. https://doi.org/10.1109/ISI.2017.8004875
[22] Ultralytics. (n.d.). YOLO architecture explained. Retrieved September 3, 2026, from https://docs.ultralytics.com/guides/yolo-architecture
[23] Ultralytics. (n.d.). Ultralytics YOLOv5 architecture. Retrieved September 3, 2026, from https://docs.ultralytics.com/yolov5/tutorials/architecture-description
[24] Wang, C.-Y., Yeh, I.-H., & Liao, H.-Y. M. (2024). YOLOv9: Learning what you want to learn using programmable gradient information. In Computer Vision - ECCV 2024. Springer. https://arxiv.org/abs/2402.13616
[25] Khanam, R., & Hussain, M. (2024). YOLOv11: An overview of the key architectural enhancements. arXiv. https://arxiv.org/abs/2410.17725

ОЦІНЮВАННЯ ТОЧНОСТІ РОЗПІЗНАВАННЯ ВІЙСЬКОВИХ ТРАНСПОРТНИХ ЗАСОБІВ НА АЕРОКОСМІЧНИХ ЗОБРАЖЕННЯХ З ВИКОРИСТАННЯМ АРХІТЕКТУР YOLO

Ph.D., Каштан В., Dr.Sci., Гнатушенко В.
Національний технічний університет «Дніпровська політехніка», Україна

Анотація. *Розпізнавання військових транспортних засобів на аерокосмічних зображеннях належить до складних задач комп'ютерного зору через малі проєкційні розміри об'єктів, складну структуру фону, часткові перекриття, варіативність просторової орієнтації та обмежену кількість репрезентативних анотованих даних. Особливу складність становить виражений дисбаланс класів, за якого інтегральні показники якості можуть не повною мірою характеризувати ефективність розпізнавання класів з обмеженою кількістю анотованих прикладів. Метою дослідження є обґрунтування вибору найбільш ефективної серед досліджуваних архітектур YOLO для розпізнавання військових транспортних засобів на аерокосмічних зображеннях за сукупністю інтегральних і покласових показників якості розпізнавання об'єктів. Дослідження виконано на сформованому власному наборі даних, що містить 2 274 аерокосмічні зображення та 11 454 анотації чотирьох класів: військові транспортні засоби, танки, вантажівки та джипи. Набір даних розподілено на 1 592 навчальні, 341 валідаційне та 341 тестове зображення. Для всіх моделей використано вхідні зображення розміром 640×640 пікселів, а тривалість навчання становила 100 епох. За сукупністю кількісних показників найбільш збалансовані результати отримано для YOLOv8: Precision становила приблизно 0,65, Recall – 0,35, mAP@50 – 0,30. Отримані результати показали, що досліджувані архітектури YOLO відрізняються за інтегральними показниками якості детектування, тоді як для класів з обмеженою кількістю анотованих прикладів характерними залишаються низькі значення повноти розпізнавання. Це свідчить про суттєву роль репрезентативності навчальних даних у забезпеченні стабільного розпізнавання окремих класів.*

Ключові слова: *аерокосмічні зображення, розпізнавання військових транспортних засобів, YOLO, глибоке навчання, детектування об'єктів, дисбаланс класів.*

UDK 004:37:001:62
DOI

CYBER-PHYSICAL COORDINATION OF AUTONOMOUS SHIPS AND SMART PORTS: A DISTRIBUTED SYSTEM-OF-SYSTEMS APPROACH

Dr.Sci., Vychuzhanin V.[1][0000-0002-6302-1832],
Ph.D., Vychuzhanin A.[2][0000-0001-8779-2503]
Odessa Polytechnic National University, Ukraine
EMAIL: [1]v.v.vychuzhanin@op.edu.ua, [2]vychuzhanin.o.v@op.edu.ua

Abstract. *This paper proposes a distributed System-of-Systems (SoS) architecture integrating Hybrid Digital Twins (HDTs) of autonomous vessels and smart ports for low-latency cyber-physical coordination. To resolve nonlinear edge-computing constraints, we combine distributed LTV-MPC with physics-informed neural networks (PINNs) for real-time hydrodynamic approximation. Concurrently, a privacy-preserving ADMM algorithm enables decentralized microgrid optimization without exposing proprietary battery data. Heterogeneous co-simulation over a 5G URLLC network demonstrates that cooperative mooring eliminates collisions, reducing maneuvering energy by 42% and stabilization time by 43%. Energy optimization yields 84.2% renewable utilization, cuts peak demand from 18.5 MW to 9.1 MW, and reduces OPEX by 45%. The study proves that stable edge coordination strictly demands end-to-end latency below 10 ms.*

Keywords: *System-of-Systems, Cyber-Physical Systems, Digital Twins, Physics-Informed Neural Networks, Distributed Optimization, Privacy-Preserving Computing, 5G URLLC.*

1 Introduction

Currently, Maritime Autonomous Surface Ships (MASS) operate as isolated cyber-physical systems (CPSs), relying on reactive, discrete legacy protocols like automatic identification system (AIS). However, safe and efficient operations in high-traffic hubs demand continuous cyber-physical synchronization between vessels and smart port infrastructure [1, 2]. The global maritime industry is undergoing a technological transformation driven by the parallel development of MASSs and smart ports [3]. The introduction of the IMO MASS Code in 2024 established the regulatory basis for highly autonomous commercial vessels employing artificial intelligence for navigation and machinery control [4, 6], while leading logistics hubs increasingly deploy 5G communications, the industrial internet of things (IoT), and DT technologies for predictive infrastructure management [5]. Nevertheless, the primary challenge has shifted from developing isolated technologies to seamlessly integrating autonomous vessels with smart ports. Vessels cannot fully leverage advanced services (e.g., Just-in-Time Arrival, automated mooring) without the continuous, high-frequency data exchange demanded by intelligent port infrastructure [3]. To address this challenge, this study proposes a distributed SoSs architecture that integrates the HDTs of autonomous vessels and smart ports. This unified cyber-physical environment actively coordinates navigation, logistics, and energy management, driving improvements in maneuvering efficiency and berthing times. Recent research increasingly explores MASS-port integration, yet reveals a distinct fragmentation across disciplines. While studies [7, 8] successfully apply DT frameworks to port sustainability and supply-chain logistics, they omit high-frequency cyber-physical

interactions. Furthermore, foundational works on automated berthing and MASS navigation [9, 10, 14] show that existing control algorithms remain predominantly vessel-centric. In these models, ships act as isolated agents, and the port serves merely as a static constraint. Concurrently, parallel decarbonization studies address cold ironing [12], urban shore-power integration [11], and renewable microgrid optimization [13]. Despite these individual advancements, current literature treats logistical, navigational, and energy domains in isolation, lacking a unified system-level architecture to synchronize them. Nevertheless, these studies generally assume deterministic vessel arrivals and centralized optimization without continuous bidirectional synchronization between onboard and shore energy systems. At the system level, study [15] identifies interoperability and standardized continuous data exchange as the principal barriers to large-scale MASS deployment. Current vessel-port synchronization lacks a unified framework, and centralized cold ironing compromises proprietary battery thermal degradation estimates (T_{FHT}). To address this, we develop a distributed SoSs architecture integrating vessel and port HDTs. Key contributions include: a 5G telecommunications model, a PINN-assisted LTV-MPC algorithm, and a privacy-preserving ADMM framework for decentralized microgrid optimization, fully verified via heterogeneous co-simulation.

2 Information and telecommunication paradigm of the SoS in the "ship–port" system

To safely transition from discrete classical ship-port interactions to continuous cyber-physical synchronization (e.g., during mooring), the communication delay (τ_d) must satisfy the following critical constraint:

$$\tau_d(t) = t_{proc} + \frac{V_{data}}{B_{channel}(\tau)} + t_{prop} \le \tau_{crit}, \quad (1)$$

where t_{proc} is the processing time at edge-computing nodes; V_{data} is the data packet size; $B_{channel}(t)$ is the dynamic bandwidth of the hybrid communication channel (5G/VDES/LEO Satcom); t_{prop} is the signal propagation delay; τ_{crit} is the maximum permissible data transmission delay for the current technological operation. Satisfying such stringent information synchronization requirements is extremely difficult within conventional coastal communication infrastructures. For the practical implementation of the proposed SoS paradigm, it is necessary to quantify the values of τ_{crit} across different interaction phases (Table 1). For dynamic port operations (e.g., automated mooring), network requirements shift fundamentally from bandwidth to strict latency minimization. These thresholds are dictated by digital control stability criteria. Under classical networked control systems (NCS) theory [16], asymptotic stability under communication delay is governed by the inequality:

$$\tau_d \prec \frac{\phi_m}{\omega_c},$$

where φ_m is the phase margin of the uncompensated system, and ω_c is the crossover frequency of the control loop. Analytically deriving the critical delay τ_{crit} requires decoupling slow vessel kinematics from fast actuator dynamics. The primary control

challenge during berthing is the rigid vessel-AMS hydraulic coupling. Specifically, suppressing vessel micromotions and destructive high-frequency actuator chattering mandates an internal force-control bandwidth ≥ 12.5 Hz. This determines the required crossover frequency of the cooperative closed-loop control system: $\omega_{crit} = 2\pi f \approx 78.5$ rad/s.

Table 1

Telecommunication infrastructure requirements for the SoS framework at different stages of port arrival

Operational phase	Type of transmitted data	Required update rate	Maximum latency (τ_{crit})	Primary communication channel
Distant approach (>50 nautical miles)	JIT profiles, ETA, meteorological data, T_{FHT} estimations	Once every 15 min	< 5000 ms	LEO Satcom (Starlink/OneWeb)
Anchorage / approach channel	Trajectories, VTS data, digital pilotage information	1 Hz	< 500 ms	VDES / 4G LTE
Berthing approach (maneuvering)	Vessel kinematics, tugboat status, depth information	10 Hz	< 50 ms	5G (port network)
Automated mooring	Port LiDAR data, mooring control commands	50–100 Hz	< 10 ms	5G URLLC / Wi-Fi 6 (LoS)

Assuming the minimum phase margin required to maintain asymptotic stability of the hydraulic system is $\phi_m \approx \pi/4$ rad (45°), the maximum permissible network transport delay is obtained analytically as: $\tau_{crit} \prec \frac{\pi/4}{78.5} \approx 0.01s$. Violating this inequality induces uncompensated phase shifts, driving actuator instability and potential collisions. Meeting this strict $\tau_{crit} < 10$ ms boundary mandates dedicated 5G port networks supporting ultra-reliable low-latency communication (URLLC). Consequently, synthesizing the distributed MPC and ADMM control algorithms requires explicitly defining the state spaces of the participating DTs whose data circulate within the SoS network .

$$x_{MASS} = \left[x, y, \phi, u, v, r, T_{FHT}^{(i)}, P_{load}, SOC\right]^T \in S_{MASS}, \quad (2)$$

where x, y, ϕ, u, v, r are the kinematic parameters (position, heading, linear and angular velocities); $T_{FHT}^{(i)}$ is the predictive estimate of the Markov time to the limiting state of critical machinery; P_{load} is the forecast power demand; SOC is the current state of charge of the onboard batteries. Accordingly, the state space of the intelligent port DT is described by the vector:

$$x_{PORT} = [traffic, depth, wind, grid, state, price]^T \in S_{PORT}, \quad (3)$$

where $traffic$ is the local shipping traffic matrix; $depth$ is the dynamic depth map (taking into account tidal variations and subsidence effects); $wind$ is the vector of hydrometeorological disturbances (τ_{env}^{port}); $grid, state$ is the energy balance of the port microgrid (including renewable energy generation); $price$ is the dynamic vector of shadow electricity tariffs. The continuous and guaranteed synchronisation of these variables (with a delay of τ < 10 ms) enables the transition to the solution of specific cyber-physical control tasks. The structural diagram of the resulting macroarchitecture Σ_{SoS} is presented in Figure 1.

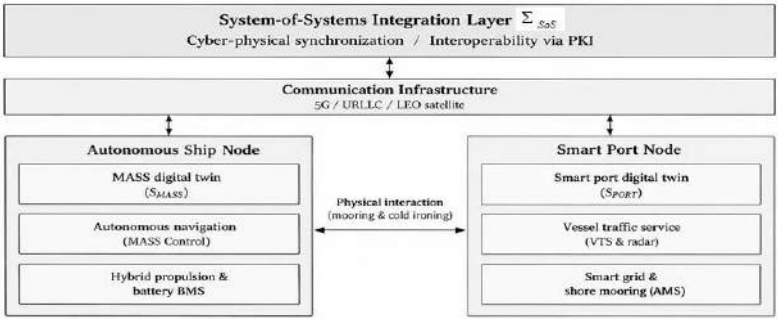


Figure 1. Macroarchitecture of the SoSs metasystem: physical, telecommunication, and cyber-physical integration of the autonomous vessel and the intelligent port.

The SoS macroarchitecture (Fig. 1) establishes the orthogonality of physical and cognitive flows. The physical layer (mooring, energy transfer) remains constrained by high inertia and nonlinear hydrodynamics, whereas the predictive integration layer (Σ_{SOS}) enables the (DTs to functionally "outrun" real time. Leveraging vessel DT predictions enables proactive port microgrid and AMS preparation. Crucially, a public key infrastructure (PKI) -based isolation of critical onboard systems (navigation, BMS) guarantees that during 5G breaches, low-level actuators remain secure. Local DTs immediately trigger safe-degradation modes, ensuring uninterrupted edge autonomy.

3 CPC of automatic mooring processes based on hybrid models

Achieving centimeter-level mooring accuracy under stochastic disturbances requires shifting from isolated onboard control to cooperative SoS execution, where the port DT actively manages shore-based AMSs. The corresponding vector-matrix equation of motion is:

$$M(\eta)\dot{v} + C(v)v + D(v)v = \tau_{ctrl} + \tau_{env}^{port} + \tau_{AMS}, \quad (4)$$

where $\eta = [x, y, \phi]^T$ is the position and heading vector in the local berth coordinate system; $v_{ctrl} = [u, v, r]^T$ is the velocity vector; *M, C, D* are the inertia, Coriolis force, and damping matrices (strongly nonlinear in shallow water and corrected by PINN models); τ_{ctrl} is the control vector of the vessel's propulsion units (azipods and

thrusters); τ_{env}^{port} is the environmental disturbance vector transmitted from the port digital twin (high-precision local data); τ_{AMS} is the attraction force vector generated by the shore-based automatic mooring systems.

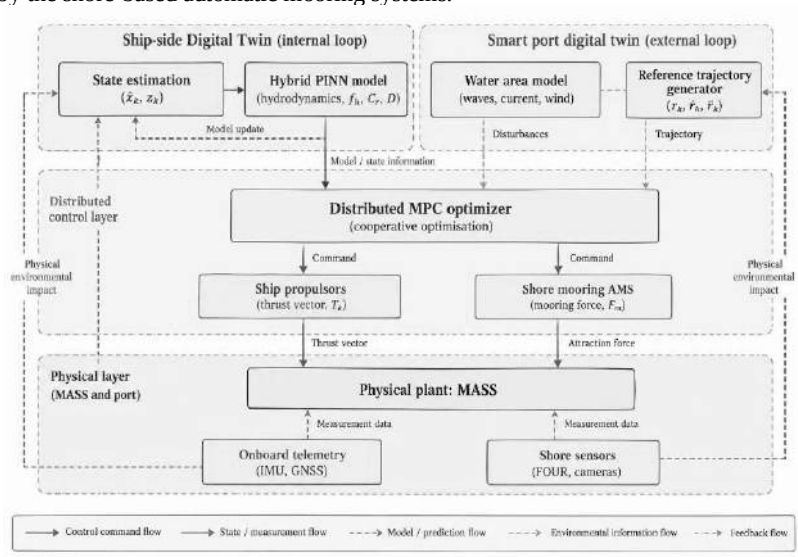


Figure 2. Structural diagram of cooperative MPC-based automatic mooring control within the SoS paradigm.

In shallow water ($T/h \to 1$), hydrodynamic matrices become highly nonlinear. To avoid static approximations, onboard PINNs with Navier-Stokes-based loss functions dynamically compute physically consistent hydrodynamic matrices (*M*, *C*, *D*) in milliseconds. The architecture decouples the outer port loop (1 Hz) and inner vessel loop (10-50 Hz) to resolve dimensionality issues. Delegating nonlinear computations to PINNs drastically reduces the MPC burden, guaranteeing control execution within the strict τ_{crit} < 10 ms latency limit. Consequently, the distributed MPC minimizes trajectory deviations while constraining control effort:

$$\sum_{k=1}^{N_p} \|\eta(t+k\,|\,t) - \eta_{ref}(t+k)\|_Q^2 + \sum_{k=0}^{N_u-1} (\|\Delta\tau_{ctrl}(t+k)\|_{R_1}^2 + \|\Delta\tau_{AMS}(t+k)\|_{R_2}^2 \quad , \qquad (5)$$

subject to the physical and spatial constraints:

$$\tau_{ctrl}^{\min} \le \tau_{ctrl} \le \tau_{ctrl}^{\max};\ 0 \le \tau_{AMS} \le \tau_{AMS}^{\max};\ v_{impact} \le v_{safe}\ ;\ N_p \cdot \eta(i+k\,|\,t) \le b_p$$

where N_p, N_u are the prediction and control horizons in discrete steps *k*; η_{ref} is the prescribed (reference) approach trajectory to the berth; *Q*, R_1, R_2 are the positive-definite diagonal weighting matrices defining the balance between positioning accuracy and the energy expenditure associated with aggressive control actions;

$\Delta\tau_{crit}$, $\Delta\tau_{AMS}$ are the increments of the control actions at the current step, the limitation of which within the objective function ensures smooth operation of the mechanisms; v_{safe} is the maximum permissible closing velocity (landing velocity), limiting the kinetic energy of fender contact and ensured through the coordinated operation of the vessel propulsion system and the shore-based vacuum grippers; N_p and b_p are the matrices and vectors defining the safe navigable corridor polytope generated by the port DT on the basis of LiDAR data. To balance navigational safety and computational efficiency, the horizons are established at N_p = 200 (providing a 20-second prediction window critically necessary to compensate for the 65,000-ton hull inertia) and N_u = 50. The weighting matrices strictly prioritize navigational safety over energy consumption. The state-error matrix $Q = diag(10^4, 10^4, 10^5)$ heavily penalizes spatial deviations. The control cost matrices are configured asymmetrically: $R_1 = diag(10^{-1}, 10^{-1}, 10^{-1})$ for vessel azipods and $R_2 = diag(10^{-3}, 10^{-3}, 10^{-3})$ for shore-based AMS. The condition $R_2 \prec\prec R_2$ algorithmically compels the optimizer to transfer the physical stabilization effort to the port network, preserving the onboard batteries. High weights in R_2 simultaneously smooth control gradients ($\Delta\tau$) to prevent destructive actuator chattering. To guarantee solvability within the telecommunication threshold (τ_{crit}<10 ms), the highly nonlinear hydrodynamic matrices $M(t)$, $C(t)$, $D(t)$ generated by the PINN model are treated as quasi-stationary over the prediction horizon N_p. This implements a linear time-varying (LTV-MPC) paradigm, effectively reducing the complex optimization to a standard quadratic programming (QP) formulation.

4 Energy integration: system-level optimization of microgrids and cold ironing technologies

The implementation of the Zero-Emission Port concept is impossible without the application of onshore power supply (OPS) technology, also known as cold ironing. The integration of MASS into the port Smart Grid requires a transition from static shore-power connection to dynamic energy-consumption optimization based on DT predictions.

4.1 Formation of the MASS DT load profile

Based on cargo loading/unloading schedules and battery charging requirements (for hybrid or fully electric vessels), the vessel DT generates a predictive power-demand profile $p_{MAS}^{pred}(t)$ for the entire berthing interval $[t_{arr}, t_{dep}]$.

4.2 Shore-side power system balancing

The digital twin of the smart port treats berthed vessels as active nodes (prosumers) within the local microgrid. The port power-balance equation at time ttt is expressed as:

$$P_{grid}(t) + P_{RES}(t) + P_{ESS_dis}(t) = P_{base_port}(t) + \sum_{i=1}^{N_{MASS}} P_{MASS_i} + P_{ESS_{ch}}(t), \quad (6)$$

where P_{grid} is the power imported from the main electrical grid; P_{RES} is the power generated from renewable energy sources (solar and wind installations located within the port area); P_{ESS_dis}, $P_{ESS_{ch}}$ are the discharge and charge power of shore-side energy storage systems; P_{base_port} is the baseline electrical load of the port (cranes, terminal facilities, and auxiliary infrastructure). The physical topology of energy flows within the ship–port system, described by this power-balance equation, is illustrated in Figure 3.

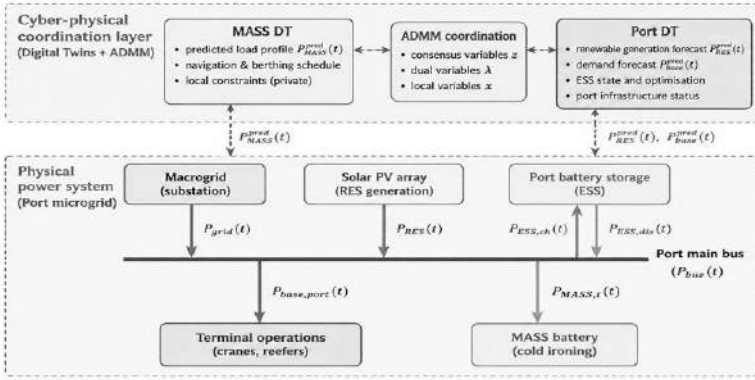


Figure 3. Structural diagram of power flow distribution in a smart port microgrid with integrated autonomous vessels (cold ironing)

In a conventional uncoordinated configuration, stochastic vessel connections (P_{MASS_i}) act as passive loads, generating transient spikes on the main bus and forcing expensive electricity imports from the utility grid (P_{grid}). The proposed SoS architecture introduces a cyber-physical coordination layer, transforming the MASS into an active prosumer. Maintaining power balance and minimizing port operational expenditures (OPEX) requires strict algorithmic synchronization of vessel charging profiles with renewable generation peaks (P_{RES}) and shore-based storage cycles (P_{ESS}). This dynamic coordination dictates the objective function for the microgrid economic dispatch.

4.3 Economic dispatch objective function

The objective of the port DT is to minimize total OPEXs and carbon emissions while satisfying the energy requirements of the fleet. The objective function Jenergy is formulated as:

$$\min J_{energy} = [C_{grid}(t)P_{grid}(t) + \lambda_{CO2} \cdot E_{CO2}(P_{grid}) + \sum_{i=1}^{N_{MASS}} C_{\deg_i}(P_{MASS_I})]dt\,, \quad (7)$$

where $C_{grid}(t)$ is the dynamic utility electricity tariff (time-of-use tariff); λ_{CO2} is the cost of greenhouse gas emission allowances (carbon tax); E_{CO2} is the emission function associated with electricity generation; $C_{\deg_i}$ is the cost function representing the thermal degradation of the battery for vessel i, quantified via

predictive T_{FHT} estimation algorithms. Minimization of the objective function is performed under strict physical and operational constraints of the microgrid. Main transformer capacity constraint (grid connection point): $P_{grid}(t) \le P_{\max}^{transformer}$.

SOC constraints for shore-side and onboard energy storage systems:

$$C_{\min} \le SOC(t) \le SOC_{\max}, \quad SOC(t+1) = SOC(t) + \frac{\eta_{ch} \cdot P_{ch}(t) - P_{dis} / \eta_{dis}}{E_{copacity}}, \qquad (8)$$

where η_{ch}, η_{dis} are the denote charging and discharging efficiencies; $E_{capacity}$ is the nominal battery energy capacity. Nonlinear power-flow constraints must regulate active and reactive power balances to prevent critical voltage sags during peak cold-ironing demand. Mathematically, the gradient of the objective function J_{energy} drives the system toward its optimal operating conditions where $C_{grid}(t) \to \min$, and $P_{RES}(t) \to \max$. To resolve the conflict between optimal microgrid dispatch and commercial data privacy (Fig. 4), we employ a distributed ADMM architecture. By exchanging only low-dimensional consensus vectors *x, z,* λ) over 5G URLLC rather than aggregating local constraints, this zero-knowledge topology guarantees asymptotic convergence to the global optimum (J_{energy}) while strictly preserving proprietary vessel parameters. Mathematically, the iterative process of decentralized ADMM optimization is based on minimizing the augmented lagrangian function and is described by the following system of recursive equations:

$$x^{k+1} = \arg\min_x L_p(x, z^k, \lambda^k),\ z^{k+1} = \arg\min_x L_p(x^{k+1}, z, \lambda^k),\ \lambda^{k+1} = \lambda^k + \rho \cdot (x^{k+1} - z^{k+1}),$$

where k is the iteration number of the data exchange process over the 5G network; $x \in X_{safe}$ is the vector of local optimization variables on the vessel digital twin side (formation of the requested power profile P_{MASS}^{pred} considering the degradation of the vessel's own batteries); $z \in Z_{grid}$ is the vector of consensus (global) variables on the port digital twin side (allocation of the available microgrid power taking into account generation capacity limits Z_{grid}); λ is the dual variables (vector of shadow electricity prices); $\rho > 0$ is the quadratic penalty parameter ensuring asymptotic convergence of the algorithm. Because the nonlinear battery degradation model creates a non-convex local objective, classical ADMM lacks convergence guarantees. We overcome this by embedding sequential convex programming (SCP) into the vessel's DT. Iteratively approximating the nonlinear function with its convex majorant guarantees convergence to a safe local optimum (KKT point). Consequently, this hybrid approach strictly satisfies all physical constraints while inherently preserving zero-knowledge privacy.

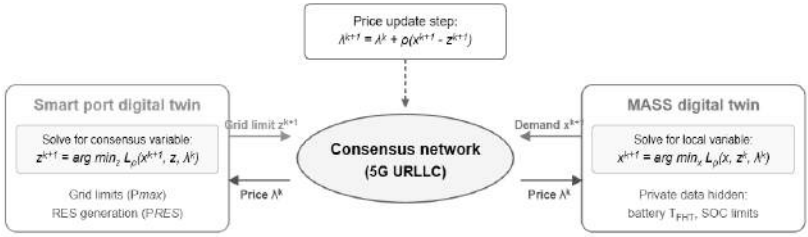


Figure 4. ADMM-based decentralized optimization architecture: system coordination of independent agents without disclosure of proprietary energy storage parameters (T_{FHT}).

5 Verification of coordinated cyber-physical interaction algorithms using co-simulation

We validated the SoS architecture using a heterogeneous co-simulation testbed (Fig. 5) that bridges two independent computational environments. MATLAB/Simulink and Python/TensorFlow handled the continuous-time MASS hydrodynamics (ODE solvers), while DIgSILENT PowerFactory executed quasi-steady-state port microgrid calculations.

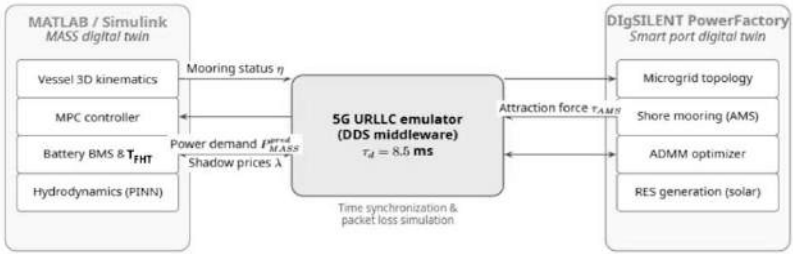


Figure 5. Architecture of the hardware-software co-simulation platform for heterogeneous DTs.

Data synchronization between these asynchronous DTs was achieved via a data distribution service (DDS) protocol over an emulated 5G network with controlled latency. To ensure numerical stability, integration utilizes the functional mock-up interface (FMI) standard, with the DDS middleware acting as the Co-Simulation Master to enforce deterministic state-vector exchange at predefined rendezvous points.Zero-order hold (ZOH) extrapolators within each DT compensate for emulated 5G transmission delays (8.5 ms) and packet losses, preventing algebraic loops and guaranteeing solver stability. By embracing edge computing, computationally intensive tasks (PINN tensor operations and nonlinear power-flow calculations) are executed locally. Only compressed macro-parameters (λ, η, τ_{AMS}, P^{pred}_{MASS}) traverse the 5G URLLC channel, ensuring latency remains within the 8.5 ms critical threshold even under peak network loads. Furthermore, this topology physically enforces the zero-knowledge privacy, as the port optimizer interacts with the vessel BMS solely via price vectors (λ) without accessing proprietary T_{FHT} data. Practical verification of this architecture was conducted using a Panamax-class autonomous container

vessel baseline scenario. The key parameters of the simulation environment are summarized in Table 2.

Table 2

Parameters of the $\sum SoS$ co-simulation environment

Model parameter	Value	Justification / Source
MASS displacement	65,000 t	Typical Panamax-class container vessel
Onboard battery capacity	8.5 MWh	Hybrid propulsion system
Shore-side AMS capacity	4 × 400 kN	Cavotec MoorMaster vacuum mooring units
Base port load	2.5 – 3.0 MW	Operation of container cranes and terminal infrastructure
Peak renewable generation	5.0 MW	Rooftop solar installations on warehouse facilities
Emulated communication delay τ_d	8.5 ms	5G URLLC latency including jitter
MPC prediction horizon (*Np*)	20 s	Sampling interval of 0.1 s

The simulation scenario covered two operational phases: final approach and mooring under stochastic crosswind disturbances of up to 15 m/s; a 24-hour port stay with connection to the microgrid under the cold ironing operating mode.

5.1 Results of automatic mooring simulation

To evaluate the robustness of the developed MPC controller under environmental uncertainty, 50 extreme worst-case scenarios were simulated using a directed Monte Carlo sampling technique. These scenarios encapsulated peak wind-wave disturbances (15 m/s crosswinds) and dynamic shallow-water squat effects. The statistical sufficiency of the sample was rigorously validated via non-parametric bootstrapping (B = 10,000), confirming that the 95% confidence interval of the expected positioning error remains strictly within the safe navigation polytope ($H_p \cdot \eta \leq b_p$). A comparison was performed between isolated control (vessel propulsion only) and coordinated SoS control (vessel + shore-based AMS). The summarized results are presented in Table 3.

Table 3

Comparative results of mooring simulations (50 monte carlo runs)

Evaluated parameter	Isolated control (vessel only)	Coordinated control (SoS: vessel + AMS)	Improvement
Maximum impact velocity (vimpact)	Exceeds vsafe in 12% of cases	vimpact < vsafe in all 50 runs	Safety guarantee
Onboard energy consumption during maneuver	142.5 kWh	82.6 kWh	42% reduction
Portion of force transferred ashore (τ_{AMS})	0% (system not engaged)	42% (distributed load sharing)	Reduced azipod wear
Vessel stabilization time at berth	14.5 min	8.2 min	43% reduction

Results in Table 3 confirm the proposed hypothesis: the hydrodynamic damping matrix dynamically corrected by the PINN model, combined with shore-based mooring mechanisms, improves maneuvering safety and mitigates azipod thrust oscillations. Delegating part of the physical control effort to the external mooring systems reduces the onboard actuation demand during maneuvering. The probability density functions (PDFs) of impact velocity from the 50 Monte Carlo runs (Fig. 6) further illustrate the different response of isolated and coordinated control under peak disturbances.

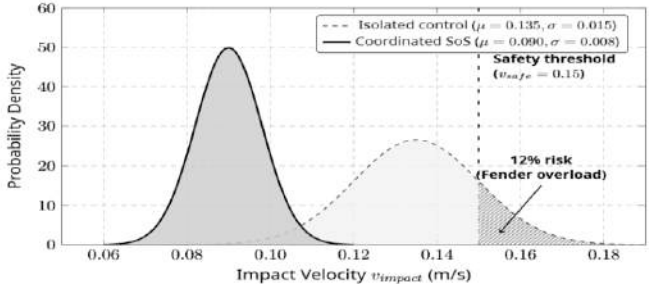


Figure 6. Probability density function curves of the approach velocity (v_{impact}) at physical contact with the berth, approximated from the results of 50 Monte Carlo simulation runs.

This results in a pronounced right-hand tail exceeding the critical threshold (v_{safe} = 0.15 m/s), creating a 12% risk of infrastructure damage. Conversely, the coordinated SoS controller shifts the operation into a safe region (median 0.09 m/s) and drastically narrows the kinematic variance (95% CI: 0.074 to 0.106 m/s). A Fisher's F-test comparing the sample variances ($F(49, 49) = 6.45$, $p = 1.2\times10^{-5}$) rigorously rejects homoscedasticity. This statistically confirms that the cooperative MPC not only reduces the expected positioning error but virtually eliminates stochastic tail risks, ensuring deterministic safety during automated berthing.

5.2 Results of decentralized energy optimization

Evaluated during the cold ironing phase, the ADMM algorithm balanced the microgrid while strictly preserving vessel data privacy. Co-simulation demonstrated rapid algorithmic convergence: the residual error satisfied the $\varepsilon = 10^{-4}$ threshold within 14 iterations. Accounting for the 8.5 ms network latency, the global optimization for a 15-minute dispatch interval computed in under 0.2 seconds. As shown in Figure 7, this decentralized dispatch restructures daily load profiles through simultaneous peak shaving and load shifting. The mathematical solution directly forces the bulk of vessel energy consumption into daytime hours, optimally aligning demand with the local photovoltaic generation curve $P_{RES}(t)$.

Table 4 consolidates the co-simulation performance metrics, demonstrating the quantitative superiority of the proposed SoS architecture over conventional power supply strategies. In the baseline non-optimized scenario (plug-and-charge), consumption mismatches trigger a critical peak demand of 18.5 MW, with renewable energy utilization reaching only 31.4%.

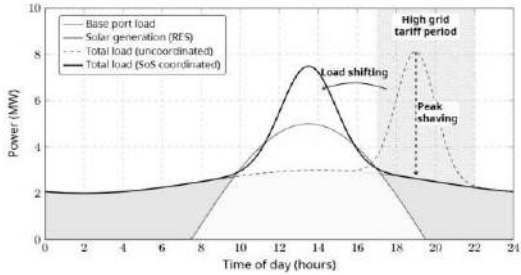


Figure 7. Dynamic balancing of the port microgrid using cognitive synchronization algorithms.

The decentralized ADMM algorithm halves peak demand (9.1 MW), boosts renewable utilization (84.2%), and reduces microgrid OPEX by 45.0% without violating onboard battery constraints. Integrating nonlinear hydrodynamics with electrical transients, this co-simulation definitively proves the cyber-physical architecture's functionality, convergence,

Table 4

Comprehensive efficiency analysis of power supply and integration strategies

Power supply scenario	Integration & control method	Peak grid load (MW)	Local RES utilization	Relative OPEX reduction compared to baseline
Isolated operation	None (onboard diesel generators only)	0.0	0.0%	Baseline
Standard cold ironing	Uncoordinated (plug-and-charge)	18.5	31.4%	Baseline OPEX (reference)
Centralized peak shaving	Heuristic (rule-based)	14.2	56.8%	18.5%
Proposed SoS architecture	Cooperative cyber-physical (ADMM)	9.1	84.2%	45.0%

5.3 Resilience to Communication Failures and False Data Injection Attacks

The results obtained in Section 5.1 demonstrate the effect of distributed vessel-port coordination under nominal communication conditions. The co-simulation was performed with an emulated communication latency of 8.5 ms, while the analytical assessment in Section 2 gives approximately 10 ms as the critical delay for the assumed actuator bandwidth and phase margin. The coordinated configuration reduced onboard energy consumption from 142.5 to 82.6 kWh and stabilization time from 14.5 to 8.2 min. In the 50 Monte Carlo scenarios, the impact velocity exceeded the adopted safe value of 0.15 m/s in 12% of the isolated-control cases, whereas no such exceedance was observed in the coordinated cases. These baseline results anchor the subsequent resilience evaluation. Instead of proposing a novel cybersecurity model, this subsection investigates how the existing cyber-physical architecture withstands degraded coordination data (i.e., delayed, missing, or unreliable information).

By decoupling local vessel control from higher-level port coordination, the architecture inherently supports graceful degradation under both communication

failures and data manipulation. When network latency exceeds the critical ~10 ms limit, the aging of external data compromises port cooperation but leaves direct vessel control intact. During such anomalies, the edge controller maintains autonomy by relying on local DT predictions and last-validated states.

However, communication availability does not guarantee information integrity; FDIA can manipulate critical variables within the MASS state vector:

$$x_{MASS} = [z, y, \phi, u, v, r, T_{FHT}^{(i)}, P_{load}, SOC]^T \quad (9)$$

Because alterations to position, velocity, or power demand directly destabilize cooperative algorithms, the architecture introduces a layer of physical redundancy. The consistency of any received state variable (y) is continuously evaluated against the local DT prediction:

$$e_{cons} = y_{resv} - y_{pred}, \quad (10)$$

where y_{resv} is the received value and y_{pred} is the baseline derived from the previous state, current control inputs, and environmental conditions.

$$e_y(k) = y^{\alpha}(k) - \hat{y}(k \mid k-1) \ , \quad (11)$$

where $y^{\alpha}(k)$ is the received value and $\hat{y}(k \mid k-1)$ is the value predicted by the local DT.

Utilizing the PINN module, the vessel cross-validates external inputs against expected physical dynamics. Substituting physically inconsistent data with local predictions immediately safeguards the control loop, entirely bypassing the need for explicit attack attribution. Consequently, the distributed architecture manages simultaneous communication degradation and data manipulation using two anomaly indicators: data age and physical consistency. Table 5 defines the three principal operating conditions derived from these criteria.

Table 5

Operational response of the distributed SoS to abnormal information conditions

Information condition	Vessel-side operation	Port-side coordination	Operational interpretation
Valid and timely information	Normal local control	Full coordination	Nominal cooperative operation
Delayed or temporarily unavailable information	Local prediction / last validated state	Reduced contribution	Degraded cooperation
Physically inconsistent information	Reject or replace affected data	Reduced or temporarily suspended update	Protection of local control

While Table 5 illustrates the core resilience paradigm—deliberately abandoning global optimality (e.g., ADMM coordination, 42% energy/43% time reductions) to enforce autonomous physical safety during anomalies—this logic requires further empirical validation. By deferring the testing of FDIA detection and severe network disruptions, the current study establishes Figure 8 as a nominal operational baseline rather than a comprehensive cyberattack profile. Consequently, evaluating the architecture via HIL execution under controlled packet loss and data manipulation remains the essential next phase of research.

5.4 Parametric assessment of cooperative-control robustness

While Sections 5.1–5.3 define nominal performance, a full systematic analysis of varied network or model uncertainties is deferred. Instead, we assess parameters within established boundaries (Table 6). For cooperative berthing, the critical analytical latency limit is ~10 ms, dictated by actuator bandwidth and phase margin (Section 2). Our co-simulation utilized an emulated 8.5 ms delay, successfully demonstrating nominal coordinated control within this boundary. Notably, this ~10 ms limit is specific to the proposed vessel–AMS configuration, not a universal MASS threshold.

Table 6

Parametric conditions and validation status for robustness assessment

Parameter	Reference condition	Assessment range	Basis of assessment	Status
Communication latency	8.5 ms	8.5–10 ms	Analytical control-stability boundary	Analytical
Critical communication delay	≈ 10 ms	—	NCS phase-margin condition	Analytical
Crosswind velocity	15 m/s	Up to 15 m/s	Existing Monte Carlo scenarios	Simulated
Communication packet loss	Not experimentally varied	—	Identified future validation parameter	Not evaluated

Validated at 8.5 ms latency via 50-run Monte Carlo simulations (15 m/s crosswinds), the coordinated architecture eliminated the 12% impact-limit (0.15 m/s) exceedance seen in isolated control. It also reduced energy consumption from 142.5 to 82.6 kWh and stabilization time from 14.5 to 8.2 min. Because the vessel retains local state access, approaching the 10 ms analytical latency limit degrades only cooperation, not direct control. This edge-autonomy yields three regions: Nominal cooperative - latency < 10 ms; full cyber-physical coordination is active; degraded cooperative - latency approaches limits; the vessel uses local DT predictions and last-known port data; local-control - network coordination is suspended; the vessel edge independently ensures physical constraints.

Figure 8 schematically maps the operating regions (communication delay vs. coordination degree). The 8.5 ms co-simulation point lies safely below the ~10 ms analytical boundary. Importantly, this ~1.5 ms separation is specific to the current vessel-AMS configuration (driven by actuator bandwidth and phase margin) and does not represent a universal MASS safety margin. Furthermore, the quantitative impacts of packet loss, cyberattacks, and hydrodynamic-model uncertainties are outside the scope of the current simulation. Instead, this analysis establishes a configuration-specific operating boundary, providing a solid baseline for future HIL experiments to test controlled network degradation and model perturbations.

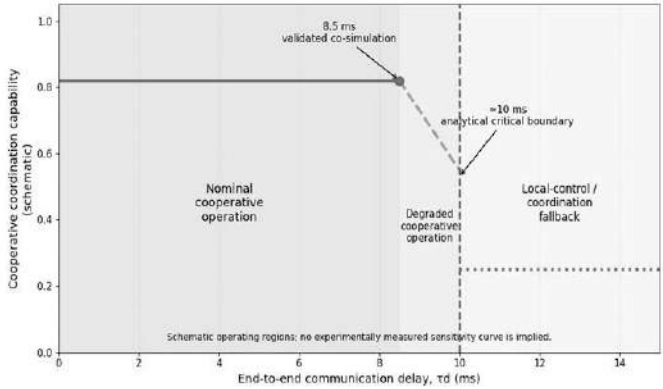


Figure 8. Analytical operating regions of the cooperative vessel–port control system as a function of communication delay.

5.5 Scalability of distributed coordination

To accommodate multi-agent traffic, the proposed SoS architecture avoids centralized computational bottlenecks by strictly separating local vessel control from distributed resource coordination. While large-scale fleet operations require future empirical validation, the architecture's scalability is analytically supported by four structural mechanisms: local computational autonomy (the vessel DT, PINN, and LTV-MPC remain on the edge);) decentralized energy management via ADMM; strict data privacy, exchanging only coordination variables while keeping T_{FHT} local; multi-rate execution, where local maneuvering operates at 10–50 Hz and port coordination runs at a lower frequency. This structural scalability is anchored by our single-MASS experimental metrics: ADMM achieved rapid convergence (residual 10^{-4} in 14 iterations; cycle <0.2 s), and the coordinated control loop operated safely at an 8.5 ms latency against the 10 ms analytical limit.

5.5.1 Computational decomposition of the distributed architecture

By decoupling individual MASS computations from shared port resources, the architecture fundamentally avoids centralized optimization bottlenecks. Each vessel's DT locally processes its PINN hydrodynamic approximations and LTV-MPC control constraints. Thus, the system scales linearly: an incoming fleet of N MASS agents introduces N independent computational nodes. Each local entity strictly isolates and retains exclusive control over its proprietary state variables, physical models, and local optimization routines. The local computational decomposition can therefore be represented as $\{C_1, C_2, ..., C_N\}$, where C_i denotes the computational subsystem associated with MASS i. The distributed coordination layer operates on the information required to couple these local subsystems with shared port resources rather than on the complete internal representation of all N vessels. This organization is particularly important for the LTV-MPC/PINN control loop because its computational frequency is substantially higher than that of the port energy-management problem. The vessel-side loop operates at 10–50 Hz, whereas the port-side coordination layer is associated with a 1-Hz operating frequency. Consequently, the addition of a vessel does not require the port-side coordination mechanism to

reproduce all high-frequency vessel-control calculations centrally. The computational hierarchy of the proposed architecture is therefore composed of three principal levels: vessel-local level, responsible for state processing, hydrodynamic prediction and LTV-MPC control; distributed coordination level, responsible for consensus, resource allocation and coordination of coupled variables; port-system level, represented by the port DT and responsible for shared infrastructure, microgrid and energy-resource constraints.

This decomposition is illustrated in Figure 9.

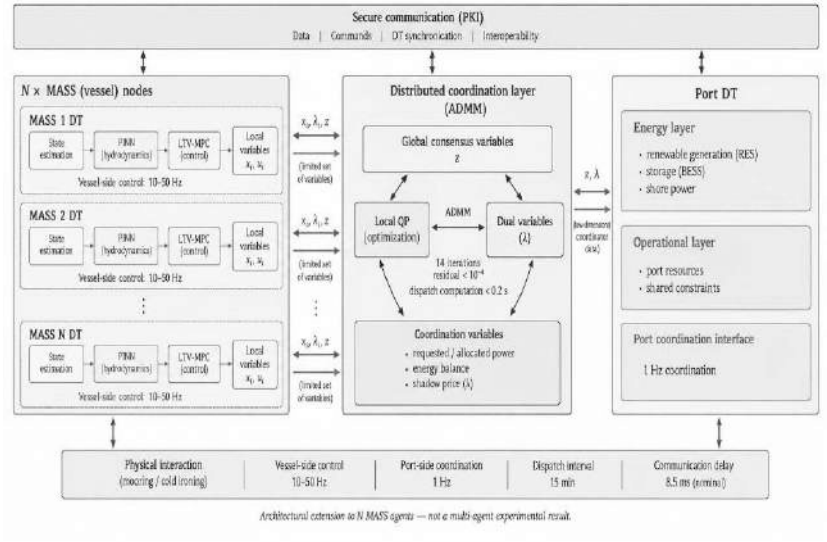


Figure 9. Distributed multi-MASS coordination architecture and computational decomposition.

The architectural diagram illustrates how the single-MASS framework structurally scales to *N* vessels. Vessel-side DTs perform local PINN/LTV-MPC functions at 10–50 Hz, exchanging only low-dimensional data with the port DT for 1-Hz global coordination (validated at 14 ADMM iterations, <0.2 s cycle, 8.5 ms delay). Crucially, the aggregate computational load for local optimizations grows linearly, $O(N)$. Although total ADMM iterations may vary depending on system coupling, this decentralized SoSs design ensures that new vessels add parallel computational tasks instead of overloading a centralized optimizer. Furthermore, this structural locality inherently guarantees edge autonomy, allowing physical vessel control to persist even during communication degradation.

5.5.2 Quantitative reference characteristics of the implemented coordination layer

The scalability assessment should be anchored to the numerical characteristics already established by the heterogeneous co-simulation. Table 7 summarizes the parameters that are directly relevant to the computational and communication scalability of the distributed coordination layer.

Table 7

Quantitative reference parameters for scalability assessment.

Parameter	Value	Origin/status	Significance for scalability	Parameter
Vessel-side control frequency	10–50 Hz	Implemented architecture	Defines the high-frequency local control layer	Vessel-side control frequency
Port-side coordination frequency	1 Hz	Implemented architecture	Defines the slower coordination layer	Port-side coordination frequency
ADMM convergence iterations	14	Co-simulation result	Reference consensus behavior	ADMM convergence iterations
ADMM residual	$<10^{-4}$	Co-simulation result	Achieved convergence criterion	ADMM residual
Dispatch interval	15 min	Co-simulation configuration	Time scale of energy coordination	Dispatch interval
Dispatch computation time	(<0.2) s	Co-simulation result	Reference computational load	Dispatch computation time
Nominal communication delay	8.5 ms	Heterogeneous co-simulation	Investigated communication condition	Nominal communication delay
Critical communication delay	≈ 10 ms	Analytical result	Boundary for the considered control-loop configuration	Critical communication delay

The measured ADMM performance (14 iterations, <0.2 s execution) establishes a computational baseline for distributed energy management. Consuming merely 0.022% of the 15-minute dispatch interval, it provides significant computational headroom, though convergence behavior may vary as fleet size increases. Similarly, the 8.5 ms co-simulation latency consumes 85% of the 10 ms analytical boundary. This leaves a configuration-specific 1.5 ms margin, which must not be interpreted as a universal safety buffer. Ultimately, these numerical references characterize the implemented optimization loop and nominal communication state, providing a rigorous baseline for evaluating future multi-MASS scalability rather than defining an absolute maximum fleet size.

5.5.3 Scaling of the communication structure

An important feature of the proposed architecture is that the distributed coordination layer does not require a fully interconnected communication topology between all MASS agents. Each vessel communicates with the coordination layer through its corresponding interface, while the shared resource constraints are resolved through the distributed coordination mechanism.

For N coordinated vessels, the number of vessel-level coordination interfaces can therefore be represented as $L_{dist} = N$. For comparison, a fully pairwise communication structure in which every MASS directly exchanges coordination information with every other MASS would require $N(N-1)/2$, The difference between these two structures becomes increasingly significant as the fleet size increases. Table 8 provides a quantitative comparison for representative values of N. The numerical values in Table 8 are derived directly from the communication topology and do not represent measured multi-MASS experiments.

Table 8

Quantitative comparison of distributed and fully pairwise communication structures.

Distributed coordination interfaces (N)	Fully pairwise relationships ($N(N-1)/2$)	Pairwise/distributed ratio
1	0	0.00
2	1	0.50
4	6	1.50
8	28	3.50
16	120	7.50
32	496	15.50

Their purpose is to quantify the structural scalability of the proposed coordination organization. For $N = 8$, for example, the distributed architecture requires eight vessel-level interfaces, whereas a fully pairwise structure would contain 28 communication relationships. At $N = 16$, the corresponding values are 16 and 120. At $N = 32$, the difference becomes 32 versus 496 relationships. Figure 10 demonstrates a critical structural advantage of the proposed architecture: coordination interfaces scale linearly (N), avoiding the bottlenecks of a fully pairwise quadratic topology ($N(N-1)/2$). While aggregate communication load still grows with fleet size, this centralized coordination topology is vital for high-traffic hubs. It allows MASS agents to dynamically enter or exit the port domain by establishing a single coordination interface, rather than requiring direct connections to every other MASS. This plug-and-play capability perfectly aligns with the SoS paradigm, where autonomous subsystems cooperate efficiently through explicitly defined, scalable interfaces.

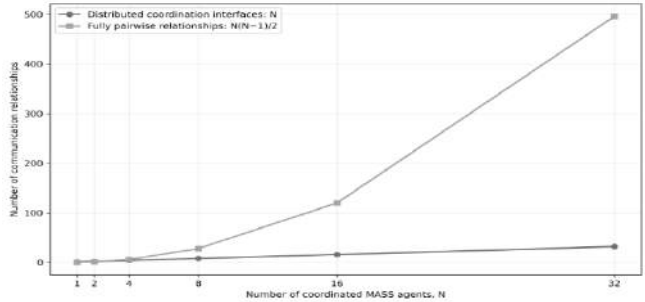


Figure 10. Structural scaling of communication interfaces: proposed linear topology (N) vs. fully pairwise quadratic architecture ($N(N-1)/2$).

5.5.4 Scalability of ADMM-based resource coordination

The second major scalability mechanism is provided by the decentralized ADMM formulation used for cold-ironing and port-microgrid coordination. The optimization problem is decomposed so that local participants retain their own technical constraints, while the coupled resource constraints are resolved through consensus. The distributed nature of this formulation has direct consequences for scalability. When an additional MASS participates in energy coordination, its vessel-side energy requirements and local constraints can be introduced as an additional local optimization problem. The existing vessel-side optimization structures do not have to be merged into a single centralized model. In general form, the distributed problem

can be considered as a set of local problems $\min_{x_i} f_i(x_i),\ i = 1,\ldots,N$ subject to the shared coordination conditions represented through the consensus variables and associated dual variables. The ADMM procedure then alternates between local optimization and consensus updates. The distributed ADMM architecture drives scalability through strict data minimization and parallel processing. Exchanging only low-dimensional shadow prices keeps proprietary models (T_{FHT}) private, eliminating the need for the port coordination layer to reconstruct full vessel states. While the baseline configuration converges rapidly (14 iterations, <0.2 s per 15-min dispatch cycle), scaling to multi-MASS fleets necessitates a strict scientific distinction: local complexity ($O(N)$) - the local optimization workload is fully distributed. Adding new MASS agents increases the number of parallel tasks linearly; global consensus - the total number of ADMM iterations required to reach consensus cannot be assumed constant and requires direct empirical validation for large fleets. This clarifies the architecture's scaling properties: it structurally guarantees linear scaling for distributed local computation, avoiding unverified claims about the overall multi-agent convergence behavior.

5.5.5 Communication load, data minimization and T_{FHT} locality

The scalability of the cyber-physical SoS architecture depends heavily on minimizing data exchange. By avoiding the transfer of complete DT representations, the vessel DT retains detailed models locally, exchanging only low-dimensional consensus variables with the port. This data-minimization strategy provides three distinct advantages: it reduces the port's aggregate communication load, eliminates the need for full vessel-specific models during optimization, and inherently preserves the privacy of sensitive metrics like T_{FHT}. While this localized execution prevents the centralized exposure of proprietary data as fleet sizes scale, it constitutes an architectural privacy mechanism rather than a complete cryptographic suite (which still requires authentication and key management). Ultimately, this approach uniquely unifies distributed computation, communication scalability, and the preservation of proprietary technical information.

5.5.6 Temporal scalability and separation of operational time scales

Another important scalability mechanism is the separation of the time scales of the individual functions. The vessel-side maneuvering controller operates at 10–50 Hz, corresponding to control periods between 0.1 and 0.02 s. The port-side coordination operates at approximately 1 Hz, while the energy-dispatch problem is evaluated over a 15-min interval. The ratio between the highest vessel-side control frequency and the port-side coordination frequency is therefore approximately 50. This means that the fastest local control loop may operate up to 50 times more frequently than the port-side coordination layer. The architecture consequently does not require every port-level coordination variable to be exchanged at the same rate as the local vessel control variables. This temporal separation is important when the number of MASS agents increases. If all vessel state variables were transmitted and processed at the highest control frequency, the aggregate communication and computational burden would increase substantially with fleet size. The proposed architecture instead retains the high-frequency functions locally and uses slower distributed coordination for shared resources. The architecture can therefore be

viewed as a hierarchical cyber-physical system in which different information classes are processed according to their operational time scales: high-frequency local vessel states and control variables; intermediate vessel–port coordination information; low-frequency energy-dispatch and resource-allocation information. This organization also contributes to resilience. As established in Section 5.3, degradation of the communication channel does not automatically eliminate the vessel-side control function because local control remains associated with the vessel subsystem. The distributed architecture can therefore reduce the degree of cooperation without immediately transferring responsibility for physical control to the communication network. The scalability consequence is that an increasing number of vessels does not necessarily require all of their high-frequency control loops to be processed centrally. The computational and communication growth is instead concentrated in the coordination functions that genuinely depend on shared resources.

5.5.7 Quantitative scalability indicators and evidence status

To avoid ambiguity between measured results and structural calculations, the principal scalability indicators are classified in Table 9. The table is important for interpreting the scientific contribution of the present subsection.

Table 9

Evidence status of the quantitative scalability indicators.

Category / Indicator	Numerical value	Evidence status	Interpretation
ADMM Convergence (Iterations / Residual)	14 / $<10^{-4}$	Experimental	Baseline convergence criterion for the implemented configuration
ADMM Timing (Computation / Interval)	<0.2 s/900 s	Experimental	Rapid execution scale; defines available computational headroom
Control Latency (Nominal / Critical / Margin)	8.5/10/1.5 ms	Experimental & Analytical	Operating boundary for the considered actuator dynamics
Topology Scaling (Distributed vs. Pairwise)	N vs, $N(N-1)/2$	Structural calculation	Demonstrates linear structural advantage over full pairwise networks
Multi-MASS Dynamics (Iteration growth, exec. time, packet-loss sensitivity)	-	Not experimentally evaluated	Complex system interactions requiring dedicated future validation

The experimentally established values demonstrate the performance of the implemented single-MASS configuration. The structural calculations quantify how the architecture changes with N. The parameters for which no values are given are deliberately identified as subjects for future validation rather than replaced with assumed numerical values. Such separation is consistent with the robustness assessment in Section 5.4, where the 8.5-ms co-simulation condition is distinguished

from the analytically derived approximately 10-ms boundary, and where packet loss and other communication degradation parameters are not presented as experimentally measured results.

5.5.8 Practical scalability limits

While structurally favorable for multi-MASS expansion, the architecture's scalability is bounded by several practical cyber-physical constraints. Computationally, the central coordination layer must still aggregate an increasing number of variables as the MASS fleet size (N) grows, and ADMM convergence rates may change under tighter multi-MASS coupling. On the network side, maintaining the nominal 8.5-ms latency requires strict resource allocation as traffic scales. Furthermore, multi-MASS operations introduce untested physical complexities, such as trajectory coupling in restricted waters, and are ultimately constrained by the finite capacity of port infrastructure (e.g., berths, shore power). Therefore, true scalability depends not just on adding autonomous MASS agents, but on the integrated capacity of the communication, computational, and physical port resources.

5.5.9 Applicability to multi-MASS smart-port operation

The presented results establish a practical structural pathway for extending the single-MASS architecture to multi-MASS operations. At the vessel level, each MASS retains its DT, PINN, and LTV-MPC, preserving edge autonomy and preventing centralized computational bottlenecks. At the coordination level, ADMM integrates new participants by resolving shared constraints via consensus variables, without centralizing proprietary technical models. At the communication level, exchanging only low-dimensional data ensures coordination interfaces scale linearly (N) rather than quadratically. Finally, the port DT manages shared physical infrastructure (e.g., shore power, grid constraints), enabling the incremental, plug-and-play integration of new MASS agents. Importantly, the multi-MASS numerical values presented in Tables 8 and 9 and Figure 11 characterize this architectural scaling framework rather than an empirical proof of a specific fleet capacity. True multi-MASS performance must be established through future dedicated experiments systematically varying the number of MASS agents, network degradation, and spatial interaction constraints.

5.5.10 Summary of scalability assessment

The scalability assessment demonstrates that the proposed distributed SoS architecture possesses several structural properties that support extension from single-MASS operation toward multi-MASS smart-port coordination. The first property is computational decentralization. Vessel-side state processing, PINN-based hydrodynamic prediction and LTV-MPC remain local to each MASS, so additional vessels introduce additional local computational entities rather than requiring complete centralization of the high-frequency control problem. The second property is distributed resource coordination. The ADMM-based energy-management mechanism separates local optimization from shared-resource consensus. The experimentally established convergence after 14 iterations with residual below 10^{-4} and execution time below 0.2 s provide quantitative reference characteristics for the implemented coordination layer. The third property is communication scalability. The number of vessel-to-coordination interfaces increases as N, while a fully pairwise architecture would require $N(N-1)/2$ communication relationships. For N=32, this corresponds to 32 distributed interfaces compared with 496 pairwise relationships.

These values are structural calculations and are not presented as measured multi-MASS results. The fourth property is temporal decomposition. The vessel-side control loop operates at 10–50 Hz, while port-side coordination operates at a lower frequency and energy dispatch is performed over a 15-min interval. This separation prevents all information from having to be processed at the highest control frequency. The fifth property is local retention of detailed DT information. The exchange of l ow-dimensional coordination variables and shadow prices avoids the need to transmit complete T_{FHT} representations, thereby supporting both communication efficiency and preservation of local technical information. Finally, the analysis identifies the principal limitations that must be addressed before claiming full fleet-scale validation: the dependence of ADMM convergence on the number and coupling of agents, network congestion under simultaneous MASS operation, packet-loss and communication-outage effects, and physical multi-vessel conflict resolution. Accordingly, the present subsection establishes a quantitatively grounded scalability assessment of the proposed architecture without introducing unsupported experimental results. The demonstrated single-MASS implementation, together with the structural N -dependent analysis, provides a scientifically justified basis for extending the architecture toward multi-agent operation. Experimental validation with increasing numbers of MASS agents remains the appropriate next step for determining the practical operating envelope of the proposed distributed coordination system.

5.6 Ablation analysis of the proposed SoS architecture

The proposed SoSs architecture integrates several heterogeneous computational and cyber-physical components, including HDTs, PINN-based hydrodynamic approximation, distributed LTV-MPC, shore-based AMSs, decentralized ADMM-based energy coordination, and the communication layer connecting vessel and port subsystems. The results presented in Sections 5.1–5.4 demonstrate the performance of the integrated architecture. The purpose of the present subsection is therefore not to repeat these results, but to examine which functional mechanisms are directly supported by the available comparative experiments and which components can only be evaluated as parts of the integrated architecture. A classical factorial ablation study would require a separate series of controlled experiments in which individual components are removed or replaced while all other parameters remain unchanged. Such a campaign was not performed in the present work. In particular, the available simulations do not contain independent experiments comparing the PINN with and without hydrodynamic correction, the proposed LTV-MPC with an alternative vessel controller, or the complete DT architecture with an equivalent centralized implementation. Consequently, no numerical contribution is assigned to these components individually. The analysis below is therefore formulated as an evidence-based ablation analysis. The experimentally evaluated alternative configurations are used to identify the contribution of the major functional mechanisms of the proposed SoS, while the components that were not independently isolated are discussed in terms of their demonstrated role in the integrated architecture.

5.6.1 Functional decomposition of the proposed SoS

The proposed architecture can be considered as a combination of three interacting functional layers. The first layer is the cooperative physical-control layer, which

combines vessel-side propulsion with shore-based AMS. Its purpose is to distribute the stabilization task between the MASS and port infrastructure during automatic berthing. The second layer is the distributed energy-coordination layer, where vessel and port energy resources are coordinated through decentralized ADMM. This layer considers vessel load demand, shore power, renewable generation, storage and shared port constraints without transferring the complete internal technical model of the vessel energy subsystem to the port optimizer. The third layer is the cyber-physical integration layer, which includes the vessel and port DTs, PINN-based hydrodynamic approximation, LTV-MPC, communication infrastructure and heterogeneous co-simulation environment. This layer provides the computational and communication framework within which the physical-control and energy-coordination mechanisms operate.

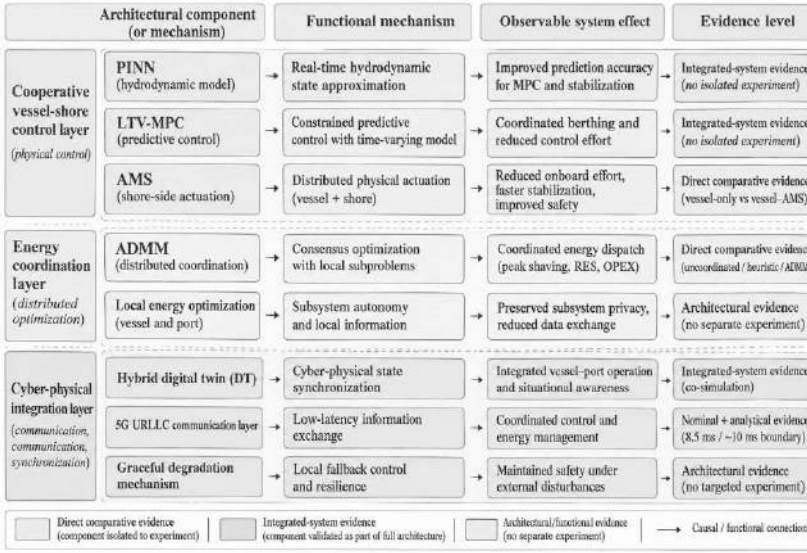


Figure 11. Evidence-based attribution of functional contributions in the proposed SoS architecture.

The distinction between these layers is important for interpretation of the numerical results. The available experiments permit direct quantitative assessment of the first two layers, whereas the individual contribution of the computational elements within the third layer is not separately identifiable from the existing experiments. Figure 11 summarizes the functional decomposition of the proposed SoS architecture in terms of the relationship between individual architectural components, their functional mechanisms, and the observable system-level effects. The decomposition is formulated on the basis of the experimental configurations and results presented in Sections 5.1–5.4, with particular emphasis on the evidence-based attribution considered in Section 5.6. As shown in Figure 11, the available evidence provides different levels of attribution for the individual architectural components. The contribution of the shore-side actuation subsystem (AMS) and the distributed

ADMM-based energy-coordination mechanism is supported by direct comparative results. In contrast, PINN, LTV-MPC, HDTs, and the communication layer were evaluated as integral elements of the complete cyber-physical configuration; therefore, their individual contributions cannot be quantitatively separated on the basis of the experiments reported in this study.

5.6.2 Contribution of cooperative vessel–shore control

The ablation analysis definitively isolates the impact of physical vessel–shore coordination from the underlying computational algorithms (PINN/LTV-MPC). By comparing isolated vessel control against coordinated automated mooring systems (AMS) across 50 Monte Carlo scenarios (15 m/s crosswinds), the architecture demonstrates a fundamental shift in control execution: performance gains - maneuvering energy dropped from 142.5 to 82.6 kWh, and stabilization time decreased from 14.5 to 8.2 min; actuation distribution - 42% of the physical stabilization effort was successfully delegated to the shore-side AMS; safety assurance - unsafe impact velocities were entirely eliminated (from a 12% risk to 0%; $F(49,49)=6.45$, $p=1.2\times10^{-5}$. Crucially, this validates that the port is not merely a passive data provider, but an active physical actuator. The transition (vessel-only control $\rightarrow$ distributed vessel–shore control) represents a structural redistribution of cyber-physical control authority, directly validating the core SoS paradigm.

5.6.3 Contribution of the shore-side physical subsystem

The preceding comparison permits a more specific interpretation of the AMS contribution. The shore-side subsystem is not introduced simply as an auxiliary safety mechanism. Its integration changes the distribution of control effort between the vessel and port. Approximately 42% of the physical control effort in the coordinated configuration is transferred to the shore-side system. This observation is consistent with the simultaneous reduction in onboard maneuvering energy and stabilization time. The vessel no longer has to compensate for the entire environmental disturbance using its own propulsion system. Part of the stabilization task is executed through the port-side actuation mechanism. The significance of this result is therefore architectural rather than merely numerical. The experiment demonstrates that the proposed SoS can exploit distributed physical resources rather than treating the vessel as an isolated cyber-physical agent. This property distinguishes the proposed architecture from a conventional MASS control architecture in which the port is external to the control loop.

At the same time, the existing experiment does not allow the separate contributions of AMS hardware and cooperative LTV-MPC logic to be quantified. Such attribution would require at least one additional controlled configuration in which the AMS is available but is not incorporated into the proposed cooperative controller. Since such an experiment was not conducted, no independent numerical contribution is assigned to the AMS algorithm or hardware beyond the experimentally demonstrated effect of the coordinated vessel–shore configuration.

5.6.4 Contribution of distributed energy coordination

The energy-management experiments (Section 5.2) provide direct comparative evidence for distributed coordination.

Table 10

Summary of SoS component contributions and attribution levels

SoS component / mechanism	Functional role in the architecture	Directly evaluated configuration	Quantitative evidence available	Attribution level	Main limitation
Hybrid digital twin (HDT)	Provides synchronized cyber-physical representation of vessel and port states	Integrated vessel–port cosimulation	Successful execution of heterogeneous co-simulation; synchronized vessel and port models	Integrated-system evidence	No independent comparison with an equivalent non-DT architecture
PINN hydrodynamic model	Real-time approximation of nonlinear shallow-water hydrodynamics for the vessel control model	PINN + LTV-MPC + coordinated AMS	Integrated maneuvering results under crosswind disturbances up to 15 m/s	Integrated-control evidence	No experiment with an alternative hydrodynamic approximation under identical conditions
LTV-MPC	Predictive constrained control of vessel motion and allocation of control effort	Vessel-side LTV-MPC with shore-side AMS	50 Monte Carlo scenarios; energy, stabilization and impact-velocity results	Direct comparative evidence for the cooperative configuration	Marginal contribution of LTV-MPC itself is not separately isolated
Shore-based AMS	Provides distributed physical actuation during automatic berthing	Isolated vessel control vs coordinated vessel–AMS control	42% of physical control effort delegated to shore-side actuation; coordinated configuration produced no unsafe cases in the 50-run sample	Direct comparative evidence	No separate experiment isolating AMS hardware from cooperative control logic
Distributed ADMM coordination	Consensus-based coordination of vessel and port energy resources	Uncoordinated, heuristic and cooperative ADMM configurations	Residual $<10^{-4}$ after 14 iterations; dispatch cycle <0.2 s; energy-management results reported in Table 4	Direct comparative evidence	Comparison does not constitute a general benchmark against all centralized/distributed optimization methods
Local vessel optimization	Preserves vessel-side computational autonomy and local model information	Distributed energy-management architecture	Local optimization combined with consensus exchange	Integrated architectural evidence	No centralized-equivalent experiment for direct computational comparison

Evaluating three strategies highlights a systematic transition in the operating regime: uncoordinated (Plug-and-charge) - 18.5 MW peak demand, 31.4% renewable

utilization; centralized heuristic - 14.2 MW peak, 56.8% renewable utilization; distributed ADMM - 9.1 MW peak, 84.2% renewable utilization, 45% OPEX reduction. These results confirm that true distributed coordination fundamentally outperforms isolated peak-shaving rules. The ADMM algorithm also exhibited rapid, stable convergence (residual $<10^{-4}$ after 14 iterations; 15-min dispatch cycle computed in <0.2 s). To clearly distinguish directly isolated effects from integrated-system evidence across all components, the architectural contributions are summarized in Table 10. As Table 10 illustrates, the strongest component-level attribution is available for the cooperative vessel–shore control and the distributed energy-management layer (ADMM). In contrast, the PINN, LTV-MPC, DT, and communication components are experimentally validated primarily as interconnected elements of the overarching architecture. Therefore, system-level performance should not be interpreted as the independently measured contribution of any single algorithm.

5.6.5 Operating-regime interpretation of the energy-management results

The energy-management results can be represented more informatively than by a numerical table alone. A useful additional visualization is a two-dimensional operating-regime map, shown schematically as Fig. 12, where the horizontal axis represents peak grid demand and the vertical axis represents renewable-energy utilization. The three experimentally evaluated configurations are then represented as individual operating points: uncoordinated plug-and-charge: 18.518.5 MW, 31.4%; centralized heuristic peak shaving: 14.214.2 MW, 56.8%; proposed cooperative ADMM: 9.19.1 MW, 84.2%.

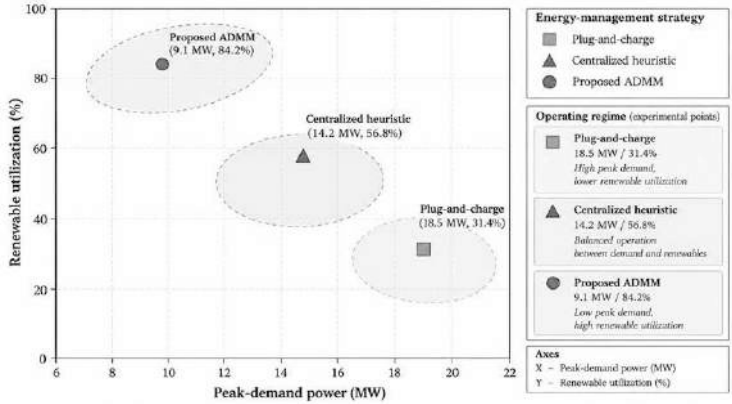


Figure 12. Operating regimes of the vessel–port energy-management strategies in the peak-demand versus renewable-utilization space.

Figure 12 complements Table 4 by representing the experimentally evaluated energy-management strategies in the two-dimensional space of peak grid demand P_{peak} and renewable-energy utilization U_{RESU}. The three operating points illustrate the system-level transition toward lower peak demand and higher renewable utilization with increasing coordination. The diagram is interpreted as an operating-regime map rather than a Pareto front, since only three configurations were experimentally

evaluated. Thus, the proposed ADMM coordination cannot be reduced to conventional peak shaving, as its effect is observed simultaneously in grid-demand reduction and renewable-energy utilization.

5.6.6 Evaluation Scope and Integrated Component Functionality

The ablation analysis evaluates the proposed architecture strictly as an integrated SoS. Instead of isolating the marginal algorithmic superiority of individual components against alternative baseline models, the study demonstrates their collective operational viability across three technical domains. Regarding cyber-physical control, the observed performance gains-including the 42% reduction in maneuvering energy - result directly from the combined execution of the digital twin, the PINN hydrodynamic model, and the LTV-MPC controller. The current experimental design confirms their joint functionality rather than independent algorithmic dominance. The energy coordination layer is assessed through the same system-level perspective. The decentralized ADMM mechanism demonstrably outperforms the evaluated uncoordinated and centralized heuristic baselines. This validates the practical efficacy of the proposed dispatch framework, avoiding unsupported claims of universal mathematical supremacy over all existing optimization solvers. At the network level, the 8.5 ms co-simulation latency verifies that the architecture can safely operate within the critical <10 ms analytical boundary. Because systematic variations in packet loss were excluded from the current test matrix, this metric serves as a nominal design constraint rather than a complete empirical robustness envelope. The present integrated evaluation thus establishes a rigorous baseline for future component-specific hardware-in-the-loop stress tests.

5.6.7 Interaction of architectural components

The SoS architecture derives its operational superiority from the interaction of distributed physical and computational resources, operating across two complementary chains. Distributed Physical Actuation (Berthing): [Disturbance → DT/PINN → LTV-MPC → {Vessel Propulsion + Shore AMS}]. The key feature is the direct branching of physical control efforts between the vessel and the smart port. Distributed Computational Coordination (Energy): [{Vessel Demand + RES + Storage + Shore Power} → Local Optimization → ADMM → Coordinated Dispatch]. The key feature is achieving global optimization without centralizing proprietary internal subsystem states.

Ultimately, Sections 5.1 and 5.2 validate that the SoS successfully unifies distributed physical execution with decentralized computational intelligence, proving that the system's value exceeds the sum of its isolated algorithms.

5.6.8 Discussion and Implications of the Ablation Analysis

The ablation analysis confirms that the architecture's operational superiority stems from system-level integration rather than the isolated impact of individual algorithmic components. The experimental evidence validates two core cyber-physical mechanisms: physical coordination, which delegates stabilization to shore-side AMS, and energy coordination, where ADMM-based optimization minimizes peak grid demand and OPEX. Practically, this establishes the port as an active control participant rather than a passive information provider, and proves that distributed coordination achieves global objectives without exposing proprietary local models (e.g., T_{FHT}).

However, a clear evidence hierarchy must be acknowledged. Because the study was not designed as a full factorial experiment, the precise marginal contributions of specific internal algorithms (e.g., PINN versus alternative hydrodynamic models, or LTV-MPC versus alternative controllers) remain analytically unresolved. Ultimately, these limitations do not weaken the validated results. Instead, they confirm the overarching SoS paradigm: performance gains arise from the unified orchestration of distributed edge intelligence, physical infrastructure, and energy resources, while deferring component-level causal attribution to future validation.

6 Discussion

Unlike existing MASS-port integration strategies [17, 18] that treat berthing as an isolated task, the proposed architecture fundamentally redistributes physical control. For example, while the safety-certified MPC in [19] ensures accurate navigation, it relies exclusively on onboard propulsion, driving up energy consumption. The SoS framework presented here circumvents this limitation by delegating physical stabilization to shore-based automated systems. This architectural shift significantly reduces onboard energy usage and actuator wear compared to conventional vessel-centric solutions.

Application of DTs. The importance of cyber-physical replicas is well-recognized; for instance, [22] established the foundations of a digital twin for the research vessel Gunnerus, while [26] developed a DT tailored for port logistics. The present work conceptually bridges these two advanced domains.

However, unlike studies focusing on independent twin deployment [22, 26], this research substantiates a co-simulation architecture where computationally intensive tasks are distributed across a heterogeneous environment, utilizing the DDS protocol as a practical time arbitrator. Decentralized energy optimization of microgrids. The application of the ADMM algorithm to port energy management was previously investigated by [20] for the allocation of electric vessels.

Parallelly, [23] demonstrated the viability of data-driven forecasting in cold ironing systems, and multimode maritime power networks were examined in recent reviews [24, 27]. Building upon these foundations, the present study introduces an essential operational condition: data confidentiality. Where our approach diverges is in the ADMM topology, which ensures the mathematical privacy of proprietary onboard parameters (such as T_{FHT}) without degrading the efficiency of microgrid dispatch.

This addresses one of the primary commercial barriers to wider Cold Ironing adoption. Telecommunication constraints. Previous works [21] and 5G Multi-Hop experiments [25] have justified the use of 5G in maritime environments, typically reporting latencies of 15 – 20 ms for remote-monitoring applications. However, the theoretical and simulation findings in this study indicate that such latencies are insufficient for a closed-loop cooperative berthing system.

The identified limit of $\tau_{rit} <$ 10 ms aligns closely with 3GPP release 17 specifications [28] for industrial control, highlighting the practical necessity of deploying private URLLC networks specifically within smart port waters. The architecture's multi-agent scalability is structurally guaranteed. The architecture scales computationally via ADMM's linear $O(N)$ complexity-resolving parallel

optimizations through lightweight shadow-price (λ) aggregation-and network-wise via dedicated 5G URLLC Physical Resource Blocks.

Future research will pivot to systemic cyber-resilience, specifically testing graceful degradation under 5G/AMS outages and zero-trust L1-estimators against FDIA to fully validate the secure SoS paradigm.

7 Conclusions

This study establishes a SoS architecture for MASS-port integration, shifting from isolated navigation to predictive cyber-physical coordination. Key validated findings include:

– cooperative control - a PINN-assisted LTV-MPC delegates physical stabilization to shore AMS. Across 50 Monte Carlo runs (15 m/s crosswinds), it eliminated collisions, reducing maneuvering energy by 42% and stabilization time by 43%;

– privacy-preserving optimization - a zero-knowledge ADMM algorithm globally balanced port microgrids without exposing T_{FHT}. It yielded 84.2% renewable utilization, halved peak demand (18.5 to 9.1 MW), and cut OPEX by 45%;

– scalability & Latency - the decentralized topology avoids quadratic complexity, ensuring linear scaling. Analytically, dedicated 5G URLLC is strictly mandated to meet the <10 ms latency threshold required to prevent actuator self-oscillations.

Future research will address systemic cyber-resilience, specifically testing graceful degradation during 5G/AMS failures and integrating Zero Trust L1-estimators against FDIAs for multi-agent hubs.

Declaration on Generative AI

AI tools (ChatGPT, Gemini) were utilized solely for text editing, translation, and illustrations. The authors strictly verified all AI-assisted content, affirm that the core research is entirely their original intellectual work, and assume full responsibility for the final article.

References

[1] N. D. Rudnichenko, V. V. Vychuzhanin, Metod upravleniya riskami sudovykh slozhnykh tekhnicheskikh sistem, Problemi tekhníki 2 (2014) 138–142.

[2] V. V. Vychuzhanin, A. V. Vychuzhanin, A hybrid model for evaluating the accuracy of failure forecasts in ship power plants, Bulletin of Cherkasy State Technological University 31 (1) (2026) 44–59. https://doi.org/10.62660/bcstu/1.2026.44.

[3] M. Elhussieny, Challenges and opportunities for autonomous vessels in the era of the smart ports, Maritime Research and Technology 4 (1) (2025) Art. 28. https://doi.org/10.21622/MRT.2025.04.1.1180.

[4] C. J. Chae, R. Baumler, Maritime Autonomous Surface Ships (MASS): Regulation, Technology, and Policy, Springer, Heidelberg, Germany, 2024. https://doi.org/ 10.1007/978-3-031-69437-0.

[5] K. X. Li, M. Li, Y. Zhu, K. F. Yuen, H. Tong, H. Zhou, Smart port: A bibliometric review and future research directions, Transportation Research Part E: Logistics and Transportation Review 174 (2023) Art. 103098. https://doi.org/10.1016/j.tre.2023.103098.

[6] Development of a Goal-Based Instrument for Maritime Autonomous Surface Ships (MASS), MSC 108/20, International Maritime Organization (IMO), London, UK, 2024.

[7] M. Zhu, C. Calderon, A. Ford, C. Robson, and J. Jin, "Digital Twin for resilience and sustainability assessment of port facility," Maritime Policy & Management, pp. 1–28, 2025, https://doi.org/10.1080/23789689.2025.2526928.
[8] R. Klar, A. Fredriksson, V. Angelakis, Digital Twins for Ports: Derived From Smart City and Supply Chain Twinning Experience, IEEE Access 11 (2023) 43236–43252. https://doi.org/10.1109/ACCESS.2023.3295495.
[9] S. Lexau, M. Breivik, A. M. Lekkas, Automated Docking for Marine Surface Vessels – A Survey, IEEE Access 11 (2023) 4697–4725. https://doi.org/10.1109/ACCESS.2023.3335912.
[10] A. S. Alamoush, A. I. Ölçer, Automated and remote engineering, maintenance, and repair in Maritime Autonomous Surface Ships (MASS), Journal of Shipping and Trade 10 (1) (2025) 1–28. https://doi.org/10.1186/s41072-025-00210-6.
[11] D. Bosich, M. Chiandone, M. Dalle Feste, G. Sulligoi, Cold Ironing Integration in City Port Distribution Grids: Sustainable electrification of port infrastructures between technical and economic constraints, IEEE Electrification Magazine 11 (1) (2023) 52–60. https://doi.org/10.1109/MELE.2022.3232965.
[12] N. N. Abu Bakar, et al., Electrification of onshore power systems in maritime transportation towards decarbonization of ports: A review of the cold ironing technology, Renewable and Sustainable Energy Reviews 178 (2023) Art. 113243. https://doi.org/10.1016/j.rser.2023.113243.
[13] N. N. Abu Bakar, J. M. Guerrero, J. C. Vasquez, N. Bazmohammadi, M. Othman, B. D. Rasmussen, Optimal Configuration and Sizing of Seaport Microgrids including Renewable Energy and Cold Ironing-The Port of Aalborg Case Study, Energies 15 (2) (2022) Art. 431. https://doi.org/10.3390/en15020431.
[14] O. M. Melnyk, O. A. Onyshchenko, Development of Computer-based Remote Technologies and Course Control Systems for Autonomous Surface Ships, International Journal of Computer Network and Information Security 22 (9) (2022) 183–188. https://doi.org/10.22937/IJCSNS.2022.22.9.27.
[15] A. S. Alamoush, A. I. Ölçer, F. Ballini, Drivers, opportunities, and barriers for adoption of Maritime Autonomous Surface Ships (MASS), Journal of International Maritime Safety, Environmental Affairs, and Shipping 8 (4) (2024) Art. 2411183. https://doi.org/10.1080/25725084.2024.2411183.
[16] S. Cuomo, Z. Jiang, Z. Wang, et al., Scientific machine learning through physics-informed neural networks: Where we are and what's next, Journal of Scientific Computing 92 (2022) Art. 88. https://doi.org/10.1007/s10915-022-01939-z.
[17] V. V. Vychuzhanin, A. V. Vychuzhanin, Digital methods and models for control and survivability of complex technical systems, Liha-Pres, Lviv–Torun, 2025, 366 p. https://doi.org/10.36059/978-966-397-556-6.
[18] N. Rudnichenko, V. Vychuzhanin, Complex Technical System Condition Diagnostics and Prediction Computerization, CEUR Workshop Proceedings 2608 (2020) 42–56. https://doi.org/10.32782/cmis/2608-4.
[19] G. Lyu, Z. Peng, J. Wang, Safety-certified parallel model predictive control of autonomous surface vehicles via neurodynamic optimization, IEEE/CAA Journal of Automatica Sinica 12 (10) (2025) 2056–2066. https://doi.org/10.1109/JAS.2024.124980.
[20] X. Sun, J. Qiu, Y. Tao, Y. Yi, J. Zhao, Distributed optimal voltage control and berth allocation of all-electric ships in seaport microgrids, IEEE Transactions on Smart Grid 13 (4) (2022) 2664–2674. https://doi.org/10.1109/TSG.2022.3161647.
[21] G. Rafiq, P. Bose, P. Orten, 5G Cellular Communication for Maritime Applications, IEEE Access (2025) 109451–109472. https://doi.org/10.1109/ACCESS.2025.3581591.
[22] H. Zhang, G. Li, L. I. Hatledal, Y. Chu, A. Ellefsen, P. Han, P. Major, R. Skulstad, A digital twin of the research vessel Gunnerus for lifecycle services: Outlining key technologies,

IEEE Communications Magazine (2022) 2–15. https://doi.org/10.1109/MRA.2022.3217745.
[23] N. N. Abu Bakar, N. Bazmohammadi, H. Çimen, T. Uyanik, J. C. Vasquez, J. M. Guerrero, Data-driven ship berthing forecasting for cold ironing in maritime transportation, Applied Energy 326 (2022) Art. 119947. https://doi.org/10.1016/j.apenergy.2022.119947.
[24] A. M. Aboelezz, B. E. Sedhom, M. M. El-Saadawi, A. A. Eladl, State-of-the-Art Review on Shipboard Microgrids: Architecture, Control, Management, Protection, and Future Perspectives, Smart Cities 6 (3) (2023) 1435–1484. https://doi.org/ 10.3390/ smartcities6030069.
[25] A. Lindenbergs, M. Muehleisen, M. Payaró, K. K. Kaare, Seamless 5G Multi-Hop Connectivity Architecture and Trials for Maritime Applications, Sensors 23 (9) (2023) Art. 4203. https://doi.org/10.3390/s23094203.
[26] K. Wang, et al., Digital twin-driven safety management and decision support approach for port operations and logistics, Frontiers in Marine Science 11 (2024). https://doi.org/10.3389/fmars.2024.1455522.
[27] S. Fang and H. Wang, Optimization-Based Energy Management for Multi-energy Maritime Grids. Singapore: Springer, 2021, https://doi.org/10.1007/978-981-33-6734-0.
[28] 3GPP TS 22.104, Service Requirements for Cyber-Physical Control Applications in Vertical Domains, Release 17, 3rd Generation Partnership Project, 2022.

КІБЕРФІЗИЧНА КООРДИНАЦІЯ АВТОНОМНИХ СУДЕН ТА «РОЗУМНИХ» ПОРТІВ: ПІДХІД НА ОСНОВІ РОЗПОДІЛЕНОЇ «СИСТЕМИ СИСТЕМ»

Dr.Sci., Вичужанін В., Ph.D., Вичужанін А.
Одеський політехнічний національний університет, Україна

Анотація. *У цій статті пропонується архітектура розподіленої «системи систем» (SoS), що інтегрує гібридні цифрові двійники (HDT) автономних суден та «розумних» портів для кіберфізичної координації з низькою затримкою. Для вирішення нелінійних обмежень периферійних обчислень ми поєднуємо розподілений алгоритм LTV-MPC з нейронними мережами, що враховують фізичні закони (PINN), для гідродинамічного наближення в режимі реального часу. Водночас алгоритм ADMM із збереженням конфіденційності дозволяє здійснювати децентралізовану оптимізацію мікромережі без розкриття конфіденційних даних про акумуляторні батареї. Гетерогенне спільне моделювання в мережі 5G URLLC демонструє, що кооперативне швартування усуває зіткнення, зменшуючи енерговитрати на маневрування на 42 % та час стабілізації на 43 %. Оптимізація енергоспоживання забезпечує 84,2 % використання відновлюваних джерел енергії, знижує піковий попит з 18,5 МВт до 9,1 МВт та зменшує операційні витрати (OPEX) на 45 %. Дослідження доводить, що стабільна координація на периферії вимагає, щоб затримка «від кінця до кінця» не перевищувала 10 мс.*

Ключові слова: *система систем, кіберфізичні системи, цифрові двійники, нейронні мережі з урахуванням фізичних законів, розподілена оптимізація, обчислення із збереженням конфіденційності, 5G URLLC.*

UDC 003.26+004.021
DOI

A VIDEO STREAM ENCRYPTION ALGORITHM THAT DOES NOT PROPAGATE ERRORS

Dr.Sci., Kovalchuk L.[1][0000-0003-2874-7950],
Dr.Sci., Hilgurt S.[2][0000-0003-1647-1790], **Ph.D., Nelasa H.**[3] [0000-0002-3708-0089]
[1,2,3]*G.E. Pukhov Institute for Modelling in Energy Engineering of the NAS of Ukraine, Ukraine*
EMAIL:[1]*lusi.kovalchuk@gmail.com,* [2]*hilgurt@ukr.net,* [3]*annanelasa@gmail.com*

Abstract. *This paper presents a resource-efficient encryption algorithm for temporary protection of video streams transmitted by unmanned aerial vehicles (UAVs) in resource-constrained environments. The algorithm uses key-dependent permutations of pixel positions defined using modular arithmetic. Within the considered transmission model, the algorithm has the error non-propagation property: corruption of one ciphertext byte affects at most one pixel in the decrypted frame. Encryption and decryption each require one pass over all pixels; therefore, their computational complexity for an $m \times n$ frame is $O(mn)$. To reduce the execution time, modulo-reduction operations are replaced with accesses to precomputed tables. The auxiliary memory required for one iteration is less than 1000000 bits. A preliminary estimate is obtained for the processing rate required to keep the total encryption and decryption time for one frame within 0.3 seconds. The intended application scenarios require protection only for a limited period, ranging from several hours to several days. The paper provides a preliminary evaluation of security against brute-force attacks and identifies statistical and structural vulnerabilities that require further investigation.*

Keywords: *video stream encryption, unmanned aerial vehicles, lightweight cryptography, error non-propagation*

1. Introduction

Cryptographic protection of a video stream transmitted by a UAV differs substantially from the protection of telemetry, control commands, or individual static images. For video encryption, the critical factors are not only the cryptographic properties of the transformation, but also the end-to-end transmission delay, throughput, amount of RAM, energy consumption, and the behavior of the system in the presence of channel errors. In [1], this problem was formulated for cases in which the operational value of intercepted data is limited by the duration of the UAV mission. In such a setting, a justified trade-off between the security level and speed is admissible, but it must rely on an explicitly defined adversarial model and an estimate of the time required for the corresponding attack.

One conservative variant of multimedia traffic protection is described by Cecchinato et al. [2], who studied the transmission of UAV audio and video data using AES. The authors showed that even for a standard primitive, the result depends on the mode of operation, channel parameters, and the nature of the stream. However, this construction does not aim to increase the speed of the algorithm, for example by reducing the number of rounds with a loss of security; it only provides a baseline, cryptographically conservative variant to which simplified solutions may be compared. In a later study, Cecchinato et al. [3] proposed an architecture for secure multimedia exchange between resource-constrained UAVs using a lightweight

implementation of AES and several synchronous keys. This work is important because it addresses real-time operation and adverse radio-channel conditions. At the same time, its result is architecture- and implementation-oriented: it does not offer a separate symmetric primitive with temporary security and a speed sufficient for image encryption. Another implementation-oriented approach is presented by Psilias et al. [4], where an FPGA architecture for protecting UAV video and telemetry based on AES is described. It demonstrates that real-time requirements can be achieved using specialized hardware. However, this does not imply the suitability of such an architecture for a simple software transformation of a frame on inexpensive onboard equipment: its delay, energy consumption, and throughput depend on the specific platform and on the way it is integrated into the transmission path. The study by Khan et al. [5] is also interesting from a methodological point of view. In that work, stream ciphers for video protection on an ARM processor are compared in terms of frame rate, throughput, cycles per byte, memory usage, and energy consumption. This approach makes it possible to compare the practical suitability of cryptographic mechanisms for protecting video data in resource-constrained systems in a comprehensive way.

The survey by Sarkar et al. [6] confirms that, for UAVs, the choice of a cryptographic mechanism should be based not only on nominal security, but also on delay, energy costs, memory, and deployability in a dynamic environment. In [7], Aljamal et al. proposed a two-layer protection scheme: an adaptive lightweight symmetric mechanism is used for the UAV-gateway channel, while a hybrid ECC-PQC approach is used for the gateway-cloud channel. These publications show the current trend toward context-dependent protection, but they do not provide a concrete solution for encrypting an intensive video stream with low onboard delay.

It should be noted that, for real-time video stream encryption, not only the speed, required memory, and cryptographic security, but also the property of error non-propagation are important. Here, error non-propagation means a property in which the distortion of one bit in the encrypted representation of a pixel after decryption may change the value of only that pixel, and not of other pixels of the frame. This criterion should be distinguished from the cryptographic security of the underlying algorithm. In synchronous stream-cipher mode or counter mode, a single error in the ciphertext does not propagate to subsequent bits of the plaintext; however, localization specifically at the pixel level requires additional assumptions about the format, packing, and synchronization of the frame. In [2-5], the use of AES and stream ciphers for protecting video data is considered, but error localization at the level of a single pixel is not the central subject of these studies.

Related directions represented in [8-10] also do not solve this issue directly: [8] proposes a multicomponent image encryption method, [9] presents an architecture for protecting small drones using public-key mechanisms, and [10] proposes an approach in the white-box model. All of them operate in a different setting and do not establish how a single distortion in encrypted data affects the matrix of the decrypted frame. The properties of SP-networks, in particular the PRESENT cipher [11] and results concerning S-boxes and the diffusion layer [12], are needed for evaluating the security of the underlying primitive, but they do not determine the nature of error propagation in a concrete mode of use.

Thus, the reviewed works do not provide a solution that would simultaneously be simple for software implementation, be lightweight and fast to compute for each frame, allow the justification of temporary security in a specified adversarial model, and ensure localization of a transmission error at the level of a single pixel.

2. Lightweight algorithm for encrypting a rectangular image with temporary security

In this section, we describe a lightweight algorithm with temporary security, intended for the encryption of a rectangular image, and having the following properties.

1. The algorithm does not propagate errors. That is, if distortions occur in the channel during ciphertext transmission and some bytes are transmitted incorrectly, then after decryption the number of incorrect bytes does not increase.

2. The target total encryption/decryption time for one frame should not exceed 0.3 seconds.

3. The amount of auxiliary memory required for implementing this algorithm should not exceed 10^6 bits, excluding the memory needed to store the image itself.

4. The algorithm is intended to provide temporary security: depending on the tasks performed and on the adversary model, the required protection time may range from 2 hours to several days.

The mathematical basis of the proposed approach is modular arithmetic: the analysis of invertibility of a mapping defined by linear formulas modulo the frame dimensions is reduced to the solvability of systems of linear congruences [13]. The universal modular transformations considered by Yang et al. [14] also show that one-to-one correspondence of a coordinate permutation is determined by the algebraic properties of its parameters. In the proposed algorithm, pixel values are not mixed: only their key-dependent permutation is performed. Therefore, if the pixel boundaries and the data order are preserved, the distortion of one bit in the encrypted representation of a pixel will change one pixel of the decrypted frame at most. Below, this approach is formalized as a family of key-dependent permutations of pixel positions in a rectangular frame.

3. Description of the algorithm

Let $V_l = \{0,1\}^l$; also, for $n \in N$, denote $[n] := \{0,1,2,...,n-1\}$. We will assume that the screen on which the image is displayed has a rectangular shape and consists of $m \times n$ pixels. Then the image will be represented as a rectangular matrix Π of dimension $m \times n$, whose elements are the pixel values π_{ij}:

$$\Pi = (\pi_{ij}),\ 0 \le i \le m-1,\ 0 \le j \le n-1, \tag{1}$$

where, depending on the image type (color or grayscale), $\pi_{ij} \in V_{24}$ or $\pi_{ij} \in V_8$.

In what follows, we identify the image with the matrix (1).

For definiteness, assume that $m \times n$, (for example, m=360 and n=420) and denote $d = \gcd(m,n)$. In our notation, the problem of constructing an image encryption algorithm that permutes pixel values can be formalized as follows. It is necessary to construct a family of transformations $\varphi: [m] \times [n] \to [m] \times [n]$, where each transformation

permutes the pixel values (that is, each of them acts on the set of their indices, $[m]\times[n]$, and is a bijection) and has the following properties:

B1) $\forall i \in [m] \quad \exists\, 0 \le j_1 < j_2 \le n-1: \quad \varphi(i, j_1) = (a_1, b_1)$, $\varphi(i, j_2) = (a_2, b_2)$, and, moreover, $a_1 \ne a_2$ (that is, the pixel values that were in one row do not necessarily fall into one row again after applying the mapping);

B2) $\forall j \in [n] \quad \exists\, 0 \le i_1 < i_2 \le m-1: \quad \varphi(i_1, j) = (a_1, b_1)$, $\varphi(i_2, j) = (a_2, b_2)$, and, moreover, $b_1 \ne b_2$ (that is, the pixel values that were in one column do not necessarily fall into one column again after applying the mapping); B3) this transformation should be specified using a relatively small amount of memory and should be computed quickly.

Each mapping from this family will be specified by a certain set of parameters (the set of such parameter tuples will be the key space). In this case, image encryption for a fixed set of parameters is performed according to the rule:

$$C = E(\Pi) = (c_{ij})_{i,j=0}^{m-1,n-1}, \tag{2}$$

where $c_{ij} = \pi_{\varphi(i,j)}$, and decryption is performed according to the rule

$$\Pi = D(C) = (\pi_{ij})_{i,j=0}^{m-1,n-1}, \text{ where } \pi_{ij} = c_{\varphi^{-1}(i,j)}, \tag{3}$$

where φ^{-1} denotes the mapping inverse to φ (it exists because, according to our requirements, the mapping φ is a bijection).

In what follows, we consider a family of mappings, each of which depends on four parameters $p,r,q,s \in [m]\times[m]\times[n]\times[n]$ (this parameter tuple is the key). Thus, for fixed $p,r,q,s \in [m]\times[m]\times[n]\times[n]$, the equality holds:

$$\varphi_{p,r,q,s}(i,j) = \big((i + pj + r) \bmod m,\ (j + qi + s) \bmod n\big). \tag{4}$$

Let us consider the encryption algorithm (2), (3), in which the mapping (4) is used. If every tuple of parameters is assumed to be admissible, then the cardinality of the key space $K = [m]\times[m]\times[n]\times[n]$ for this encryption algorithm is $|K| = (m \cdot n)^2$. For small values of m,n, this value may be insufficient even for temporary security: for example, fo m=360 and n=420 we obtain $|K| = 360^2 \cdot 420^2 = 22861440000 \approx 1.33 \cdot 2^{34}$, which approximately corresponds to a 34-bit key. If, according to the computational capabilities of the adversary, such security is insufficient, then two or more full or partial iterations of this mapping can be performed (for example, one iteration with four parameters and one with two parameters), each time with different key parameters. However, we next show that not all parameter tuples are admissible, since the mapping is not bijective for all such tuples. Let us consider and analyze one iteration. First, we need to formulate the condition under which the mapping (4) is bijective.

Proposition 1. The mapping (4) is bijective if and only if the system of congruences

$$\begin{cases} x + py \equiv 0 (\bmod m); \\ y + qx \equiv 0 (\bmod n), \end{cases} \quad (5)$$

has the unique solution (0,0) on the intervals $-(m-1) \le x \le m-1$, $-(n-1) \le y \le n-1$.

Proof. First note that the domain and the codomain of the mapping (4) are finite and have the same cardinality. Therefore, bijectivity of this mapping is equivalent to its injectivity. Assume that, for two distinct pairs, (x_1, y_1) and (x_2, y_2), the equality $\varphi_{p,r,q,s}(x_1, y_1) = \varphi_{p,r,q,s}(x_2, y_2)$ holds. This means that the following system of equalities holds:

$(x_1 + py_1 + r) \bmod m = (x_2 + py_2 + r) \bmod m$ and $(y_1 + qx_1 + s) \bmod n = (y_2 + qx_2 + s) \bmod n$,

which is equivalent to

$$\begin{cases} (x_1 + py_1) \bmod m = (x_2 + py_2) \bmod m; \\ (y_1 + qx_1) \bmod n = (y_2 + qx_2) \bmod n. \end{cases}$$

Let $x = x_1 - x_2$ and $y = y_1 - y_2$. Then the latter system is equivalent to the system

$$\begin{cases} (x + py) \bmod m = 0; \\ (y + qx) \bmod n = 0. \end{cases}$$

Then the condition $(x_1,y_1) \neq (x_2,y_2)$ is equivalent to the condition that the system

$$\begin{cases} (x + py) \bmod m = 0; \\ (y + qx) \bmod n = 0, \end{cases}$$

has a nonzero solution on the intervals $-(m-1) \le x \le m-1$, $-(n-1) \le y \le n-1$, and the proposition is proved. Note that the condition in Proposition 1 must be checked for every generated key. This condition restricts the key space and, accordingly, reduces its cardinality.

In particular, for the parameters m=360 and n=420, the cardinality of the key space is approximately 2^{32}, which is equivalent to a 32-bit key (rather than 34 bits, as in the case of selecting parameters without restrictions). Thus, the key space is reduced, but not very significantly.

It is important to note that the bijectivity condition itself does not give a convenient analytical formula for the inverse mapping needed for decryption. However, decryption can be performed without computing the inverse mapping. That is, if encryption is performed according to the rule $c_{ij} = \pi_{\varphi(i,j)}$, $0 \le i \le m-1$, $0 \le j \le n-1$, (according to (2)), then for decryption it is sufficient for all $0 \le i \le m-1$, $0 \le j \le n-1$, to perform the following steps: 1) compute $\varphi(i, j)$; 2) set $\pi_{\varphi(i,j)} = c_{ij}$. This decryption method is correct due to the bijectivity of the function φ for each fixed key. Thus, for correct decryption it is sufficient to verify the bijectivity of the selected mapping; the next step is to optimize its computation.

4. Optimization of computations

Since the mapping (4) contains resource-consuming reduction modulo operations (in fact, division with remainder), without optimization such an algorithm is practically impossible to use in a resource-constrained environment. Therefore, we

analyze the possibility of increasing the speed of the algorithm by adding an additional amount of memory that will store certain intermediate computation results.

Let, for the mapping $\varphi_{p,r,q,s}(i,j)=\big((i+pj+r)\bmod m,\,(j+qi+s)\bmod n\big)$ the key data $p,r,q,s\in[m]\times[m]\times[n]\times[n]$ be fixed. With these key data fixed, let us construct two tables, T_p and T_q, each having two rows whose entries depend on the parameters p and q, respectively. In the table T_p, the upper row consists of the numbers from 0 to n-1, that is, all values that the variable j can take; the lower row consists of the values $t_p(j)=(p\cdot j)\bmod m$. In table T_q, the upper row consists of the numbers from 0 to m-1, that is, all values that the variable i can take; the lower row consists of the values $t_q(i)=(q\cdot i)\bmod n$. With this notation, mapping (4) can be rewritten as

$$\varphi_{p,r,q,s}(i,j)=\big(\big(i+t_p(j)+r\big)\bmod m,\,\big(j+t_q(i)+s\big)\bmod n\big). \tag{6}$$

Using tables T_p and T_q, the computations on the right-hand side of (6) can be performed as follows, without division with remainder:

$$\big(i+t_p(j)+r\big)\bmod m=\begin{cases} i+t_p(j)+r, \text{ if } & i+t_p(j)+r<m;\\ i+t_p(j)+r-m, \text{ if } & m\le i+t_p(j)+r<2m;\\ i+t_p(j)+r-2m, \text{ if } & i+t_p(j)+r\ge 2m. \end{cases} \tag{7}$$

Indeed, since each of the values $i,\,t_p(j),\,r$, by definition, lies between 0 and m-1, their sum is always strictly less than 3m; therefore, the computations on the right-hand side of (7) are valid.

Similarly,

$$\big(j+t_q(i)+s\big)\bmod n=\begin{cases} j+t_q(i)+s, \text{ if } & j+t_q(i)+s<n;\\ j+t_q(i)+s-n, \text{ if } & n\le j+t_q(i)+s<2n;\\ j+t_q(i)+s-2n, \text{ if } & j+t_q(i)+s\ge 2n. \end{cases} \tag{8}$$

Thus, both coordinates of the image of a pixel can be computed without performing division with remainder, using tables, additions, and at most two subtractions of the corresponding modulus. We can then estimate the amount of auxiliary memory required for this acceleration.

5. Memory size

To estimate the memory size, consider one frame of size 360x420 pixels, that is, mn=151200 pixels. If the image is stored in grayscale and one byte is allocated per pixel, then one frame requires 151,200 bytes, or 1,209,600 bits. For a color image in RGB format with three bytes per pixel, 453,600 bytes, or 3,628,800 bits, are required. Therefore, if the image buffer itself is taken into account, the memory size is determined primarily by the frame size, not by the auxiliary data of the algorithm. The key of one iteration consists of four numbers $p,r\in[m]$ and $q,s\in[n]$. For m=360 and n=420, each of these numbers can be encoded by 9 bits, since $2^8<420<2^9$. The minimal memory size for the key is 36 bits. In a practical implementation, it is convenient to store these parameters in 16-bit unsigned variables; then the key of one iteration occupies 64 bits, that is, 8 bytes.

For optimized computation of the mapping, two tables are used. The upper rows of the tables do not have to be stored, since they coincide with the array indices; it is

sufficient to store only the values $t_{P(j)}$, $j \in [n]$, $t_{q(i)}$, and $i \in [m]$. Each value is less than $\max\{m,n\} = 420$; therefore, 9 bits are sufficient for theoretical storage. Thus, the memory size for the tables is $(m+n)\cdot 9 = 780 \cdot 9 = 7020$ bits, that is, approximately 878 bytes. In an implementation using 16-bit words, the tables occupy $2(m+n) = 1560$ bytes, or 12,480 bits.

Thus, the auxiliary memory for one iteration, that is, the key and two tables, even in a 16-bit implementation is approximately 1568 bytes. This is much less than 10^6 bits. After estimating the auxiliary memory, it remains to determine the processing speed required for real-time processing of one frame.

6. Running time

In the naive implementation, formula (4) contains two reduction modulo operations for each pixel. After the tables T_p and Tq are constructed, these operations are replaced by memory accesses and several additions, comparisons, and subtractions. This is why precomputing the tables is important for a lightweight implementation of the algorithm.

For one frame, mn=151200 pixels have to be processed. One encryption operation performs one pass over all pixels. Decryption can be performed by an analogous pass, computing, for each initial position, its encrypted position and copying the corresponding value from the encrypted image back. Therefore, the total number of positions processed during encryption and decryption of one frame is $2mn$=302400 pixels. For the total encryption and decryption time not to exceed 0.3 seconds, the average processing time per position must be no more than $0.3/(2mn) \approx 9.9 \cdot 10^{-7}$ seconds, that is, approximately $1\,\mu s$ per pixel. For a one-byte image, this corresponds to processing approximately 1 megapixel/s; for an RGB image, it corresponds to copying approximately 1.8 MB of data in 0.3 seconds, without accounting for memory-management and control overhead.

This estimate does not experimentally confirm that the 0.3-second bound is achieved. It only indicates the order of processing speed required from an implementation. The actual running time depends on the processor architecture, cache, memory-access speed, frame-storage method, and pixel format. Therefore, this estimate is preliminary and requires experimental verification on the target hardware platform.

7. Security against brute-force attack

Consider a brute-force attack for one iteration under the assumption that the adversary knows the frame size and the general structure of the algorithm, but does not know the parameters p, r, q, s. If the whole parameter space is considered, then for m=360 and n=420, we have $|K| = (mn)^2 = 22861440000 \approx 2^{34.4}$. As noted above, for a strict cryptographic estimate, only admissible keys should be taken into account, for which the corresponding mapping is bijective. Therefore, the value given above should be regarded as an estimate of the full parameter space of one iteration.

If the adversary can test R keys per second, then the approximate time of exhaustive search is $T = |K| / R$. For example, for $R = 10^5$ keys/s we obtain approximately 63.5 hours, for $R = 10^6$ keys/s approximately 6.35 hours, and for $R = 10^7$ keys/s, approximately 38 minutes. The 2-hour threshold corresponds to a speed of about $3.2 \cdot 10^6$ keys/s. Thus, one iteration can provide two-hour security against simple brute force only against an adversary with moderate computational capabilities and without a more efficient way to test the correctness of the key.

If temporary security for several days is required, or if the adversary model allows a much higher key-testing speed, one iteration is insufficient. In this case, it is advisable to apply two or more independent iterations with different key parameters, as well as to limit the lifetime of one key. At the same time, it should be taken into account that for structured transformations, attacks faster than brute force may be possible; therefore, the estimate $|K|$ alone is not a complete estimate of cryptographic security. Thus, a brute-force attack provides only the first and simplest level of security evaluation. Next, attacks that may exploit statistical properties of images or the structure of the mapping itself must be considered separately.

8. Other attacks

A brute-force attack is not the only relevant attack for such an algorithm. The considered transformation only permutes the pixel values and does not change the values themselves. Therefore, the brightness or color histogram of the image is preserved. For some classes of images, for example frames with large homogeneous regions, a horizon, a road, sky, buildings, or typical contours of objects, even after pixel permutation there may remain statistical features that help the adversary recognize the type of scene or partially recover its structure. Known-plaintext attacks should be considered separately. If the adversary has at least one pair consisting of a plaintext image and the corresponding encrypted image under the same key, they obtain information about the permutation of pixel positions. For images with many repeated values, this may not recover the entire permutation at once; however, for a specially chosen test image with unique or nearly unique pixel labels, the permutation can be recovered much faster. Therefore, in the temporary-security model, it is desirable to explicitly assume that the adversary cannot conduct a chosen-plaintext-image attack. For video streams, an additional source of information is the similarity of neighboring frames. If the same key is used for many consecutive frames, the adversary can accumulate statistics over several frames and use temporal correlations in the video. This is especially dangerous for scenes in which the camera or objects move slowly. Therefore, the key parameters should be updated regularly, and the number of frames encrypted under one key should be limited. Another possible threat is related to the structure of the mapping (4) itself. It depends only on four numerical parameters and has a linear modular form in the pixel coordinates. If the adversary manages to establish a correspondence between a sufficient number of positions in the plaintext and encrypted images, they can obtain a system of modular relations for the parameters p, r, q, s. Such an attack may be significantly faster than brute force. Thus, the security of the algorithm cannot be justified solely by the size of the parameter space; it is also necessary to restrict the adversary model and to

experimentally test how recognizable different classes of images remain after permutation. At the same time, these limitations do not mean that the algorithm cannot be useful in practical scenarios. Its use can be considered admissible in cases where the UAV is in constant motion and consecutive frames of the video stream change substantially due to changes in camera position, viewing angle, object scale, lighting, or background. In this regime, the adversary does not obtain a long sequence of almost identical images from which the structure of the permutation could gradually be recovered or stable scene contours could be used. The admissibility of this approach is additionally increased if the key parameters are changed frequently, for example after a fixed number of frames or after short time intervals. Thus, this algorithm should be considered a means of temporarily masking a video stream under limited computational resources, rather than a universal algorithm for the cryptographic protection of images. Its most natural area of application is scenarios in which the adversary has only passive access to the transmitted video stream, cannot obtain pairs of plaintext and encrypted frames under the same key, and the usefulness of the intercepted information decreases rapidly over time. In contrast, for static images, repeated scenes, video from a fixed camera, or prolonged use of the same key, this algorithm may be insufficient, since pixel permutation does not completely destroy the statistical and geometric structure of the image. These considerations define the limits of applicability of the algorithm and naturally lead to the formulation of the model limitations.

9. Model limitations

The estimates of running time and memory given above are preliminary. They are based on counting elementary operations and the amount of auxiliary data, but they do not take into account all features of the real UAV hardware platform: processor frequency, cache memory, memory bandwidth, frame format, method of access to the video buffer, energy consumption, and interaction with other processes. Therefore, a final conclusion about the practical applicability of the algorithm requires experiments on real hardware platforms or on platforms as close as possible to real ones. The error non-propagation property also has clear limits of applicability. It holds for the model in which the encrypted image is transmitted as a sequence of independent bytes or pixel components, and corruption of an individual byte does not change the syntax of the entire stream. If, before or after transmission, compression, packetization, coding with inter-frame dependencies, or another format is used in which an error in one bit can affect the decoding of a larger fragment, then the error non-propagation property must be verified for the entire transmission system, not only for the pixel permutation. In addition, the described transformation by itself does not ensure authenticity or integrity of the data. If the adversary intentionally changes, deletes, or permutes bytes of the encrypted stream, the algorithm can localize the consequences of individual distortions, but it does not detect the fact of active interference. Protection against an active adversary requires additional mechanisms for integrity control and authentication. Thus, the proposed approach should be regarded as a lightweight algorithm for temporary protection or masking of video data within a clearly defined model: short key lifetime, limited computational capabilities of the adversary, no access to chosen plaintext images, and transmission of frames in a format compatible with the error non-propagation requirement. The final evaluation

of the viability of the algorithm should include not only theoretical calculations, but also experimental measurements of time, memory, energy consumption, and the quality of visual masking on real video streams.

10. Experimental results

Below, we present a simple numerical experiment for a rectangular image of size 360x420 pixels. The image was specially constructed as an illustrative test example: a field, trees, and a person. The purpose of the experiment is to show the appearance of the image after one iteration of the permutation algorithm and to examine the algorithm's behavior when part of the encrypted frame is corrupted.

Table 1

Initial experimental parameters

Parameter	Value
Frame size	360×420 pixels
Number of pixels	151 200
Grayscale image size, 1 byte per pixel	151,200 bytes = 1,209,600 bits ≈ 147.7 KiB
Color RGB image size, 3 bytes per pixel	453,600 bytes = 3,628,800 bits ≈ 443.0 KiB
Parameters of one iteration	p=6, q=7, r=37, s=91
Mapping	$\varphi(i,j)=\big((i+pj+r)\bmod 360,(j+qi+s)\bmod 420\big)$

In this example, the parameters p=6 and q=7 are used. For a frame of size 360×420, they satisfy the following simple sufficient conditions for bijectivity of the mapping: $p=6u$, $q=7v$, $uv \bmod 5 \neq 3$. Here $u=v=1$; therefore, $uv \bmod 5 = 1 \neq 3$. Hence, the corresponding mapping is a bijection, and decryption uniquely recovers the original image.

11. Case without transmission distortion

If encryption is performed according to the rule $c_{ij}=\pi_{\varphi(i,j)}$, decryption can be performed without explicitly computing φ^{-1}, using the rule $\pi_{\varphi(i,j)}=c_{ij}$, by iterating over all $i\in[m]$, $j\in[n]$. Thus, both encryption and decryption require a single pass over all image pixels. The number of mapping computations for one frame equals the number of pixels, namely 151,200. Let us give an example of encrypted and decrypted images. Let the original image (plaintext) be shown in Fig. 1. After encryption using the parameters specified above, the image shown in Fig. 2 is obtained.



Figure 1. Original image

If no distortion occurs during transmission of the encrypted image, decryption yields an image that is identical to the original.

12. Case with distortion of the encrypted image

To verify the error non-propagation property, corruption of the encrypted frame was simulated. The image shown in Fig. 1 was used as the original image. The corresponding ciphertext was therefore identical to that shown in Fig. 2. It was then assumed that interference occurred during transmission, resulting in the corrupted ciphertext shown in Fig. 3. For illustration, a contiguous 20×20-pixel block in the encrypted image was modified. Thus, 400 pixels of the encrypted image were corrupted in the channel. Since the image was an RGB image, this corresponded to 1,200 modified bytes.

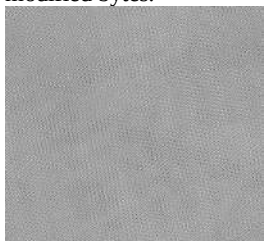


Figure 2. Encrypted image after one iteration of the pixel permutation

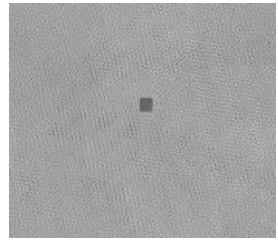


Figure 3. Encrypted image with an intentionally corrupted 20×20-pixel block

After decryption, the number of pixels that differed from the original image was also 400. The number of modified bytes after decryption was also 1,200. Thus, in this experiment, the corruption did not propagate: each corrupted pixel of the encrypted frame caused exactly one pixel to be corrupted after decryption.

Table 2

Numerical values of the metrics for the example with corrupted ciphertext

Metric	Value
Size of the simulated corrupted region in the encrypted frame	20×20 pixels
Number of corrupted pixels in the encrypted image	400
Number of corrupted bytes in the encrypted RGB image	1,200
Number of incorrect pixels after decryption	400
Number of incorrect bytes after decryption	1,200

The image obtained by decrypting the corrupted ciphertext is shown in Fig. 4. The error mask is shown in Fig. 5.



Figure 4. Image obtained by decrypting the corrupted ciphertext



Figure 5. Error mask after decryption: red dots indicate incorrect pixels

13. Experimental conclusion

The example confirms two basic properties of the algorithm. First, with the selected bijective parameters, the pixel permutation is reversible, and decrypting an uncorrupted ciphertext reproduces the original image exactly. Second, an error in the encrypted frame does not propagate to neighboring pixels after decryption: the number of incorrect pixels after decryption equals the number of corrupted pixels in the encrypted frame. At the same time, after one iteration, the image may still retain certain visual features of the original scene. Therefore, for practical application of the algorithm to video streams, it is advisable to consider multiple permutation iterations, frequent changes of key parameters, or use of the algorithm only in scenarios in which the UAV is in constant motion and consecutive frames change substantially.

14. Conclusions

This paper proposes an algorithm for encrypting video streams based on a key-dependent permutation of pixel values in a rectangular image. For the family of transformations used in the algorithm, a bijectivity condition is formulated that ensures correct decryption. Encryption and decryption can be performed without explicitly computing the inverse mapping; their computational complexity is $O(mn)$. The proposed construction also does not propagate transmission errors: distortions of individual ciphertext bytes should not increase the number of distorted bytes after decryption. At the same time, the problem of evaluating the cryptographic security of the proposed algorithm cannot be considered fully solved.

This paper considers only security against exhaustive search over the key parameters, which is determined by the size of the set of admissible keys. Such an estimate is necessary, but by itself it does not exclude the existence of more efficient attacks that exploit the structure of the transformation or the properties of the encrypted data. In particular, the possibility of statistical attacks related to the redundancy of natural images remains an open question. Distributions of brightness and color values, correlations between neighboring pixels, the presence of edges, homogeneous regions, and local patterns may potentially contain information that an adversary can use to recover part of the permutation or to filter out key parameters. In this sense, there may be a certain analogy with the cryptanalysis of a simple substitution cipher, where statistical properties of natural language make it possible to substantially narrow the set of possible keys.

However, the existence of such attacks against the proposed algorithm, their practical feasibility, and the amount of data required have not yet been established. Future research should be directed toward constructing a formal adversarial model and analyzing attacks that use the statistics of individual frames and correlations between consecutive frames of the video stream. Attacks with known or chosen plaintext, as well as possible structural attacks on the family of permutations, also require separate analysis. Only after such an analysis will it be possible to draw a justified conclusion as to whether the algorithm provides the claimed temporary security not only against exhaustive search, but also against other possible methods of cryptanalysis.

It should be noted that the error non-propagation property of the proposed algorithm characterizes only the frame model and does not replace the analysis of

cryptographic security, in particular, security against attacks that may exploit redundancy or correlations in video data.

15. Acknowledgements

The authors gratefully acknowledge the financial support provided by the National Research Foundation of Ukraine for this study, which was carried out within the framework of Project No. 2025.07/0204, "Secure jamming-resistant system for transmitting video information from an unmanned aerial vehicle," state registration No. 0125U003164.

16. Declaration on Generative AI

During the preparation of this work, the authors used Gemini for grammar and spelling checks. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

[1] Kovalchuk, L., Davydenko, A., Klymenko, T., Nedashkivska, A., Hilgurt, S., Development of an Algorithm with Temporary Cryptographic Security for Encrypting Video Stream from an Unmanned Aerial Vehicle. Eastern-European Journal of Enterprise Technologies (2025), 5(9(137)), 41-53. https://doi.org/10.15587/1729-4061.2025.340917.

[2] Cecchinato, N., Toma, A., Drioli, C., Oliva, G., Sechi, G., Foresti, G.L., A Secure Real-Time Multimedia Streaming through Robust and Lightweight AES Encryption in UAV Networks for Operational Scenarios in Military Domain. Procedia Computer Science (2022), 205, 50-57. https://doi.org/10.1016/j.procs.2022.09.006.

[3] Cecchinato, N., Toma, A., Drioli, C., Oliva, G., Sechi, G., Foresti, G.L., Secure Real-Time Multimedia Data Transmission from Low-Cost UAVs with A Lightweight AES Encryption. IEEE Communications Magazine (2023), 61, 5, 160-165. https://doi.org/10.1109/MCOM.001.2200611.

[4] Psilias, D., Milidonis, A., Lentaris, G., Voyiatzis, I., Secure Video and Telemetry FPGA Architecture for UAVs. In Proceedings of the 2024 9th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Preveza, Greece, 20-22 September (2024); pp. 69-74. https://doi.org/10.1109/SEEDA-CECNSM63478.2024.00021.

[5] Khan, M., Dagenborg, H., Johansen, D. Performance Evaluation of Lightweight Stream Ciphers for Real-Time Video Feed Encryption on ARM Processor. Future Internet (2024), 16, 261. https://doi.org/10.3390/fi16080261.

[6] Sarkar, S., Shafaei, S., Jones, T.S., Totaro M.W., Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques. Drones (2025), 9, 583. https://doi.org/10.3390/drones9080583.

[7] Aljamal, M., Khassawneh, B.S., Alsarhan, A., Okour, S., Almusfar, L.A., AlThani, B.F., Aldossary, W., A Novel Dual-Layer Quantum-Resilient Encryption Strategy for UAV-Cloud Communication Using Adaptive Lightweight Ciphers and Hybrid ECC-PQC. Computers (2026), 15, 101. https://doi.org/10.3390/computers15020101.

[8] Belazi, A., Migallón, H. Drone-Captured Wildlife Data Encryption: A Hybrid 1D-2D Memory Cellular Automata Scheme with Chaotic Mapping and SHA-256. Mathematics (2024), 12, 3602. https://doi.org/10.3390/math12223602.

[9] Ozmen, M.O., Yavuz, E., Dronecrypt - An Efficient Cryptographic Framework for Small Aerial Drones. In Proceedings of the 2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29-31 October (2018); pp. 1-6. https://doi.org/10.1109/MILCOM.2018.8599784.

[10] Yang, Y., Dong, H., Li, Z., Xiao, S. A Lightweight White-Box Encryption Device with CARX Algorithm for Secure Image Transmission. Journal of King Saud University - Computer and Information Sciences (2023), 35, 101727. https://doi.org/10.1016/j.jksuci.2023.101727.

[11] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C. PRESENT: An Ultra-Lightweight Block Cipher. In Cryptographic Hardware and Embedded Systems - CHES 2007, Vienna, Austria, 10-13 September (2007); Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4727, pp. 450-466. https://doi.org/10.1007/978-3-540-74735-2_31.

[12] Heys, H.M., Tavares, S.E. Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis. Journal of Cryptology (1996), 9, 1-19. https://doi.org/10.1007/BF02254789.

[13] Koblitz, N. A Course in Number Theory and Cryptography, 2nd ed.; Graduate Texts in Mathematics; Springer: New York, NY, USA, 1994. https://doi.org/10.1007/978-1-4419-8592-7.

[14] Yang, X., Yu, X., Zou, Q., Jia, J., Image Encryption Algorithm Based on Universal Modular Transformation. Information Technology Journal (2010), 9, 680-685. https://doi.org/10.3923/itj.2010.680.685.

АЛГОРИТМ ШИФРУВАННЯ ВІДЕОПОТОКІВ, ЯКИЙ НЕ РОЗПОВСЮДЖУЄ ПОМИЛКУ

Dr.Sci., Ковальчук Л., Dr.Sci., Гільгурт С., Ph.D., Неласа Г.
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Україна

Анотація. *У статті представлено малоресурсний алгоритм шифрування для тимчасового захисту відеопотоку безпілотного літального апарата (БПЛА) в умовах обмежених обчислювальних ресурсів. В алгоритмі використовуються залежні від ключа перестановки позицій пікселів, побудовані на основі модульної арифметики. Алгоритм має властивість непоширення помилок: пошкодження одного байта шифротексту спричиняє зміну не більш ніж одного пікселя після розшифрування. Обчислювальна складність шифрування та розшифрування кадру розміром m×n становить O(mn). Для прискорення обчислень операції редукції за модулем замінено зверненнями до таблиць попередньо обчислених значень. Обсяг додаткової пам'яті для однієї ітерації становить менше ніж 1000000 біт. Отримано попередню оцінку швидкості оброблення даних, необхідної для того, щоб сумарний час шифрування та розшифрування одного кадру не перевищував 0.3 секунди. Алгоритм орієнтований на тимчасовий захист даних на період від кількох годин до кількох днів. У роботі наведено попередню оцінку його стійкості до атаки повного перебору та визначено напрями подальшого дослідження статистичних і структурних уразливостей.*

Ключові слова: *шифрування відеопотоку, безпілотні літальні апарати, малоресурсна криптографія, непоширення помилок*

UDC 004.94
DOI

CONDITIONAL GENERATIVE MODELS WITH SYNTHETIC DATA QUALITY CONTROL FOR RECOGNITION OF UNDERREPRESENTED CATEGORIES OF MEDICAL IMAGES

Mikhalev K. [1][0009-0007-8058-4569], **Ph.D., Nikolenko A.** [2][0000-0002-9849-1797]
Odesa Polytechnic National University, Ukraine
EMAIL: [1]kirill.mikhalev.9035@gmail.com, [2]anatolyn@ukr.net

Abstract. *This article addresses the problem of class imbalance, which is one of the key limitations in building image recognition systems in computer vision applications. The imbalance between classes, in which some diagnostic categories are represented by thousands of samples, while others contain only a few dozens, leads to a systematic bias of models towards dominant classes and a complete inability to recognize rare pathologies, which is unacceptable in a clinical context. The article covers methods of synthetic data generation based on conditional generative-adversarial networks, mechanisms of selective filtering of synthetic samples, as well as strategies for adaptive sample balancing using a median target level of class representation. Special attention is paid to the selective filtering mechanism as a key scientific contribution of the work, which distinguishes the proposed approach from existing balancing methods based on generative models. The results demonstrate that the proposed method provides a significant improvement in balanced accuracy and macro-averaged F1-score compared to the baseline model. In addition, the study shows that the combination of conditional image generation with two-criteria filtering of synthetic samples allows to achieve a significant level of recognition for all minority classes.*

Keywords: *class imbalance, generative-adversarial networks, image generation, selective filtering, image recognition*

Problem Statement.

Rapid development of machine learning and computer vision methods in image recognition tasks are becoming increasingly relevant in various subject areas, in particular in medicine, security, autonomous transport and multimedia data analysis.

Significant progress in this area is associated with the use of convolutional neural networks, which demonstrate high accuracy rates provided that there are large and qualitatively balanced training samples. However, in practice, such samples are often unbalanced, which manifests itself in a significant advantage of some classes over others. Data imbalance negatively affects the process of training models, since algorithms tend to focus on dominant classes, ignoring less represented ones. This leads to a deterioration in the generalization ability of models and a decrease in the quality of classification for minority classes, which is critical in many practical applications. Existing approaches to solving this problem, such as oversampling, undersampling, and classical data augmentation, have certain limitations, in particular, insufficient diversity of generated examples or loss of important information.

Analysis of Previous Studies.

Image recognition remains one of the central problems in computer vision, with continued progress driven by increasingly sophisticated architectures – from convolutional networks to transformer-based models such as the Vision Transformer

[1]. Transfer learning has become the dominant paradigm for applying these architectures to medical image classification, where labeled data is scarce and expensive to obtain [2], [3]. However, the effectiveness of any such model remains fundamentally constrained by the quality and structure of the training data. One of the most persistent obstacles in practical applications is class imbalance, where the number of examples differs substantially across categories. Recent broad reviews confirm that this problem continues to bias models toward dominant classes and degrade generalization on minority categories, despite considerable methodological progress over the past decade [4], [5]. Classical resampling approaches remain a common baseline. SMOTE, which generates synthetic minority examples through interpolation [6], continues to be combined with modern deep architectures; for instance, SMOTified-GAN integrates SMOTE-generated candidates with a GAN refinement stage to correct their unrealistic distribution [7]. Nevertheless, purely interpolation-based methods are known to struggle with complex, high-dimensional image distributions. A more expressive alternative is offered by generative adversarial networks, originally proposed by Goodfellow et al. [8], which allow complex data distributions to be modeled directly. The conditional variant introduced by Mirza and Osindero [9] extended this framework to allow class-controlled generation, forming the basis of most subsequent GAN-based balancing methods. A recent survey specifically focused on GAN applications to imbalance problems in computer vision confirms that GAN-based oversampling now constitutes one of the most active branches of the field [10], while a broader systematic mapping study covering more than 3,000 papers highlights healthcare as one of the primary application domains [11]. Recent architectural refinements continue to appear, such as oversampling schemes that combine bootstrap resampling with Wasserstein GAN training to stabilize generation for minority classes [12]. This happens because interpolation-based methods only mix existing samples together and cannot create truly new visual patterns. Generative adversarial networks, in contrast, learn the actual distribution of the data, which allows them to generate more realistic and diverse minority-class examples than interpolation alone. Despite these advances, indiscriminate use of synthetic samples remains a recognized weakness of GAN-based balancing: several recent studies note that low-quality or misclassified synthetic examples can be as harmful as the imbalance they are meant to correct, motivating confidence-weighted or classifier-guided filtering of generated data before it enters the training set [13].

This concern is echoed by emerging work on diffusion-based generation, which has recently been shown to improve downstream classification accuracy when applied to natural [14] and medical images alike [15], including dedicated studies on skin disease image synthesis [16]. The HAM10000 dataset has become a standard benchmark for evaluating class-imbalance techniques in dermatological image analysis, and several recent studies specifically target its imbalance using attention mechanisms [17] or classical machine learning and CNN comparisons [18]. Beyond dataset-specific solutions, more general oversampling frameworks continue to be proposed for imbalanced deep learning classification [19], and derived, rebalanced variants of established benchmarks have also been released to facilitate fairer comparison across methods [20].

Unresolved Issues.

Despite this growing body of work, the combination of conditional generative modeling with an explicit, quality-aware filtering mechanism – rather than unconditional acceptance of all generated samples – remains comparatively underexplored, which is the gap addressed in this paper.

Objective of the Article.

In this context, a promising direction is the use of generative models, in particular conditional generative adversarial networks (cGANs), which allow synthesizing new data taking into account belonging to a specific class. This article considers an approach to balancing unbalanced samples by combining generative modeling and classical augmentation methods. Particular attention is paid to the experimental analysis of the impact of synthetically generated images on the quality of training recognition models, which allows to assess the feasibility and effectiveness of the proposed approach for image recognition tasks.

Main Content.

This paper proposes a comprehensive method to solve the problem of classifying unbalanced images, which is based on the integration of conditional generative adversarial networks and a mechanism for selective selection of synthetic data. The main idea is that not only the quantity, but also the quality of synthetically generated images significantly affects the efficiency of training classification models. The proposed method combines three key components: conditional image generation, synthetic data reliability assessment, and adaptive class balancing. This combination allows not only to equalize the distribution of classes, but also to minimize the negative impact of noisy or low-quality synthetic samples.

Image generation. Let the training sample be given

$$A = (x_i, y_i)_{(i=1)}^{N}, y_i \in \{1, ..., K\} \quad (1)$$

where x_i – images, y_i – corresponding class label, K is the number of classes. In the case of unbalanced sampling, the distribution of the number of samples across classes is uneven

$$N_k = |\{x_i : y_i = k\}|, \exists k, j : N_k << N_j \quad (2)$$

the goal is to construct a new sample A′ in which the class imbalance is reduced

$$A' = A \cup A_{gen} \quad (3)$$

where A_{gen} is the set of synthetically generated images.

To generate synthetic images, a conditional generative adversarial network is used, which consists of a generator G and a discriminator D. A generator is defined as

$$G : (z, y) \to x, z \sim p_z(z) \quad (4)$$

where z is a random noise vector drawn from a prior distribution $p_z(z)$ – typically normal distribution and y is a conditional variable representing the target class.

Discriminator estimates the probability that the image is real

$$D : (x, y) \to [0,1] \quad (5)$$

optimization is performed as

$$\min_G \max_D L_{cGAN}, \quad (6)$$

where L_{cGan} – is a loss function.

Synthetic data reliability assessment**.** Unlike traditional approaches, in which all generated images are added to the training set, the proposed method introduces a quality-based selection mechanism. A pre-trained classifier is used to assess the quality, which determines the probability of an image belonging to the class

$$s = \max_k P(y = k \mid x_{gen}), \quad (7)$$

where P is the probability, given by the pre-trained classifier, that the generated image x belongs to class k. k simply refers to one of the K classes in the dataset.

The sample is formed according to the condition

$$x_{gen} \in A_{gen} \quad if \quad s \geq \tau, \quad (8)$$

where τ is a quality threshold. Thus, only those images that the classifier identifies with high confidence are added to the training sample.

Adaptive class balancing**.** Instead of completely equalizing the number of samples across classes, an adaptive strategy is used. Let

$$N_{target} = median(N_1, N_2, ..., N_k) \quad (9)$$

the number of samples generated for each class is

$$M_k = max(0, N_{target} - N_k) \quad (10)$$

This avoids oversaturation of the sample with synthetic data and reduces the risk of overfitting. The proposed Class-Aware Selective cGAN approach is implemented as a sequential multi-step process that combines the generation of synthetic data, its evaluation and further use for training the classification model. The algorithm is designed in such a way as not only to compensate for the imbalance of classes, but also to ensure the high quality of additional data introduced into the training sample. At the first stage, the initial dataset is analyzed to determine the degree of imbalance between classes. For each class, the number of available samples is calculated, which allows to distinguish dominant and minority classes. The information obtained is used to form the target balancing parameters, in particular, to determine the required number of synthetic images for each underrepresented class. The second stage involves training a conditional generative adversarial network. The cGAN model is trained on the initial dataset using class labels as conditional information. During the training process, the generator gradually approaches the distribution of synthetic images to the real distribution for each class, while the discriminator improves the ability to distinguish between real and generated examples. An important feature is that the generation takes place taking into account the class, which provides control over which samples are created. At the third stage, synthetic images are generated for minority classes. The volume of generated data is determined based on a preliminary imbalance analysis. The fourth stage is key to the proposed method and distinguishes it from most existing approaches. It consists in the selective selection of synthetic images based on their quality. For this, a pre-trained classifier is used, which evaluates each generated image and determines the probabilities of its belonging to each class. Based on these probabilities, a confidence indicator is calculated – the maximum probability among all classes. Next, a threshold selection rule is applied: only those

images for which the confidence value exceeds a given threshold are included in the final set of synthetic data. Thus, samples with artifacts, distortions, or an uncertain structure that could negatively affect the training process are filtered out. This stage allows you to significantly improve the quality of the formed sample and reduce the risk of overtraining. At the fifth stage, a new training sample is formed by combining the original data with the selected synthetic images. In this case, an adaptive balancing strategy is used, which assumes that the number of samples in each class does not necessarily have to be the same. Instead, a target level of class representation is determined, for example, based on the median value, and generation is performed only until this level is reached. This approach avoids excessive use of synthetic data and preserves the natural structure of the distribution. At the final stage, the final classification model is trained on the formed balanced sample. By combining real and high-quality synthetic data, the model is able to better learn the features of minority classes, which leads to increased classification accuracy and improved generalization ability. Thus, the proposed algorithm is an integrated system that combines generative modeling, data quality assessment, and adaptive balancing. Unlike traditional approaches, where synthetic data is used without additional control, this method implements a mechanism for their selection, which allows to increase the efficiency of using generative models in the classification problems of unbalanced data. The diagram of the proposed algorithm is shown in Figure 1.

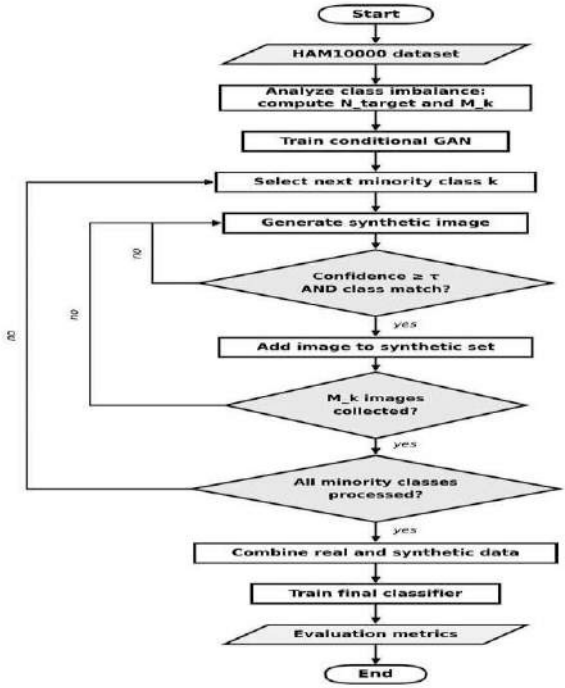


Figure 1. The algorithm diagram of proposed method.

In this work, the HAM10000 dataset is used for experimental studies, which is one of the most representative datasets in automated dermatological diagnostics. This dataset contains more than 10,000 dermatoscopic images of skin lesions collected from various sources, including clinical databases and medical archives. All images are annotated and belong to seven different classes corresponding to the most common types of pigmented skin lesions, including melanoma, melanocytic nevi, basal cell carcinoma, and other pathologies. An important characteristic of this dataset is a significant imbalance between classes: some categories are represented by thousands of examples, while others contain only a few hundred or even fewer images.

Experiments

Such uneven data distribution reflects the real conditions of medical practice, where rare diseases are much less common than common ones, which complicates the construction of effective classification models. In addition, the images in the dataset are characterized by significant variability in resolution, illumination, scale, and background conditions, which further increases the complexity of the recognition task. This makes HAM10000 a suitable test environment for evaluating data balancing methods, in particular approaches based on generative models. The use of this dataset allows not only to verify the effectiveness of the proposed method in conditions of real imbalance, but also provides the opportunity to compare it with existing scientific works in which it is widely used. Thus, the choice of HAM10000 is justified from the point of view of both practical significance and scientific relevance of the study [21]. To evaluate the effectiveness of the proposed method, two experimental configurations were considered: a baseline model replicating the approach from the reference Kaggle implementation [22] and the proposed Class-Aware Selective cGAN (CAS-cGAN) pipeline. Both configurations were evaluated on the same held-out test set, and the comparison was performed using three metrics: overall classification accuracy, balanced accuracy, and macro-averaged F1-score. The use of balanced accuracy and macro-averaged F1-score is particularly important in the context of class-imbalanced data, as these metrics give equal weight to each class regardless of its size. The baseline model was designed to replicate the standard approach commonly applied to the HAM10000 dataset in the existing literature and public implementations. It consists of a custom convolutional neural network trained directly on 28×28 pixel grayscale-encoded images without any class balancing strategy. The baseline architecture comprises three convolutional blocks, each consisting of a convolutional layer with ReLU activation, max-pooling, and batch normalization, followed by dropout regularization. The final classification head consists of a fully connected layer with 256 units and a softmax output layer with 7 units corresponding to the seven diagnostic categories. The model was trained using the Adam optimizer with a learning rate of 0.001 and categorical cross-entropy loss. Training was performed for up to 25 epochs with early stopping (patience = 5) and learning rate reduction on plateau (factor = 0.5, patience = 3). Batch size was set to 64. It is important to note that the baseline model was trained on the original unbalanced training subset without any oversampling, undersampling, or synthetic data augmentation. This configuration reproduces the conditions under which class

imbalance has the most pronounced negative effect, particularly on minority classes. Class distribution by samples quantity illustrated in Figure 2.

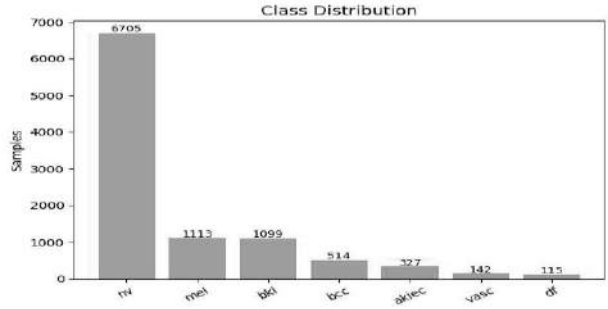


Figure 2. HAM10000: distribution of images by classes and samples.

The imbalance ratio between the largest class (nv, 6,705 images) and the smallest (df, 115 images) is 58.3:1, making the standard classification accuracy a very unreliable indicator of model quality. The proposed approach addresses the class imbalance problem through a multi-stage pipeline combining conditional generative modeling, high-quality filtering of synthetic samples, and transfer-learning-based classification. Each component of the pipeline is designed to interact with the others, and it is this interaction that determines the overall effectiveness of the method. Imbalance Analysis and Generation Planning. The first stage of the pipeline involves a systematic analysis of the training subset to quantify the degree of imbalance between classes. The training set has the following class distribution: nv – 5,364 images, mel – 890, bkl – 879, bcc – 411, akiec – 261, vasc – 113, and df – 92. Instead of a naive strategy of aligning all classes to the largest size – which would require generating over 5,000 synthetic images for the most underrepresented categories and risk overloading the training set with artificial data – the proposed method uses the median class size as the target balancing level. The median value for the training set is 411 images, corresponding to the bcc class. For each class whose number of examples falls below this median, a difference is calculated, which determines the required number of synthetic images: for mel – 0 (already exceeds the median), for bkl – 0, for bcc – 0, for akiec – 150, for vasc – 298, for df – 319. Classes that have already reached or exceeded the target value are left unchanged. This adaptive planning step ensures a controlled and proportional volume of generated data, reducing the risk of overfitting on synthetic patterns. Training a Conditional Generative Adversarial Network. The generative component of the pipeline is a conditional generative adversarial network – a type of deep generative model capable of synthesizing images given a given class label. Unlike standard GANs, which generate images without any control over their content, the conditional version receives information about the desired class at both the generator and discriminator stages, enabling the production of samples that are not only visually realistic but also class-specific. The generator is trained to transform random noise vectors of dimension 128 into plausible 64x64 pixel skin lesion images for a given diagnostic category, while the discriminator learns to distinguish real images from generated ones, simultaneously checking for class matching.

Both networks were trained jointly in adversarial mode for 300 epochs with a batch size of 64, using a variety of stabilization techniques to prevent instabilities common to GAN optimization. Specifically, the Least Squares GAN loss was used instead of the standard binary cross-entropy, label smoothing was applied to the discriminator targets (real labels were set to 0.9 instead of 1.0), and the generator was updated twice for each discriminator update step to prevent the latter from converging too quickly. Both models were optimized using the Adam algorithm with $\beta_1 = 0.5$. All images were processed at a resolution of 64×64 pixels, which provides significantly more visual information compared to the 28×28 pixel format used in the baseline model. Selective filtering is a key contribution. The distinctive element of the proposed method and its main scientific contribution is the selective filtering mechanism applied to the generated images before they are included in the training set. This step addresses a fundamental limitation of existing GAN-based balancing approaches: generated images are uneven in quality, and indiscriminately including all synthetic samples can introduce noise, artifacts, and mislabeled examples, which degrades rather than improves the classifier's performance.

The filtering procedure works as follows. A separate classifier, pre-trained on the original real data for 20 epochs, independently evaluates each generated image. This classifier, based on the EfficientNetB0 architecture with weights pre-trained on ImageNet, achieved 81.3% accuracy on real data, making it a reliable evaluator of the quality of synthetic samples. For a generated image to be accepted into the extended training set, two conditions must be simultaneously met: first, the maximum predicted class probability must exceed the confidence threshold $\tau = 0.8$; second, the class predicted with the highest confidence must match the target class for which the image was generated. The threshold value was determined empirically through preliminary experiments: several candidate values (0.6–0.9) were evaluated on a held-out subset of generated images, and $\tau = 0.8$ provided the best trade-off between retaining a sufficient volume of synthetic samples and excluding low-confidence or visually inconsistent generations. Samples that do not satisfy at least one of these conditions are discarded. In the experiments, the percentage of accepted samples ranged from 62% to 89% depending on the class: the highest acceptance rates were observed for the vasc (89%) and bcc (84%) classes, while for akiec and df, they were 62% and 67%, respectively, reflecting differences in the generator's ability to synthesize convincing examples for each lesion type. Following filtering, a total of 634 synthetic images out of 1,100 generated were added to the training set, corresponding to an average acceptance rate of 57.6%.

Dataset formation and training of the final classifier**.** After filtering, the accepted synthetic images were combined with the original real training data, forming a final extended training set of 8,646 images. The class distribution in this combined dataset is significantly more balanced compared to the original: the imbalance ratio decreased from 58.3:1 to 13.1:1. While this ratio still reflects a degree of imbalance, it represents a 4.5 fold reduction relative to the original distribution, which is sufficient to substantially improve recognition of minority classes without requiring full equalization, which would risk oversaturating the dataset with synthetic samples.

Results and discussion

Before moving on to a detailed analysis, it's important to note a significant difference in the evaluation conditions of the two methods. The Kaggle implementation of the baseline model was tested on a sample of 201 images, while the proposed CAS-cGAN method was evaluated on a stratified test sample of 2,003 images generated with a fixed random seed. The smaller test sample size in the baseline method reduces the statistical reliability of the obtained estimates: it ranges from 5 to 22 samples, making the precision and recall values for these classes unstable and sensitive to random partitioning. In terms of overall accuracy, the baseline model achieves 0.80, while the proposed method achieves 0.73. However balanced accuracy for proposed method is 0.67, while baseline one is around 0.35.

This is where the key problem with standard accuracy as a metric for imbalanced data emerges. The nv class in the Kaggle sample accounts for 142 of the 201 samples, or approximately 71% of the test set. The high accuracy (total not balanced) of the baseline model is explained by its predictive accuracy for almost all input images, yielding a recall of 0.95 for this class. However, for the other six classes, the recall averages only 0.45. The proposed method presents a different picture: despite its lower overall accuracy, the macro-average F1-score is 0.65 versus 0.56 for the baseline model. That is, by a metric that equally considers all classes, the proposed method outperforms the baseline by 0.09. Detailed accuracy report is shown in Figure 3.

```
Metric              Baseline    CAS-cGAN    Delta
Accuracy:           0.7094      0.7324      +0.0230
Balanced Accuracy:  0.3170      0.6743      +0.3573
Macro F1:           0.3437      0.6490      +0.3053
============================================================

[CAS-cGAN] Classification Report (Test Set):
              precision    recall  f1-score   support

       akiec       0.52      0.52      0.52        65
         bcc       0.51      0.75      0.61       103
         bkl       0.47      0.71      0.56       220
          df       0.81      0.57      0.67        23
          nv       0.94      0.77      0.85      1341
         mel       0.42      0.58      0.49       223
        vasc       0.88      0.82      0.85        28

    accuracy                           0.73      2003
   macro avg       0.65      0.67      0.65      2003
weighted avg       0.79      0.73      0.75      2003
```

Figure 3. Accuracy report of proposed method.

For the akiec class, the proposed method achieves an F1-score of 0.52 versus 0.46 for the baseline model, and the result is estimated using 65 samples versus 5 for the baseline model, making the resulting estimate significantly more statistically reliable. For the bcc class, the F1-score increases by 0.16 – from 0.45 to 0.61 – with a significant increase in recall from 0.50 to 0.75, indicating the detection of a significantly higher proportion of real basal cell carcinoma cases. For the bkl class, the F1-score increases from 0.51 to 0.56 with an increase in recall from 0.45 to 0.71.

Two classes deserve special attention. The df class is completely absent from the Kaggle notebook test set – not a single sample of this rarest class was included in the test, which in itself is a serious methodological flaw. The proposed method is evaluated on 23 df samples and achieves an F1-score of 0.67, a significant result for the class with the least representation in the dataset. For the mel class, the baseline

model demonstrates a precision of 1.00 with a recall of only 0.40 – in other words, it predicts melanoma extremely rarely, and missing 60% of real-world cases is clinically unacceptable. The proposed method provides a more balanced result: a recall of 0.58 with an F1-score of 0.49.

Notably, mel already exceeded the median target before balancing (890 training images) and therefore received no synthetic augmentation. Its comparatively modest gain is better explained by the residual dominance of the majority class nv (5,364 images even after balancing): since mel and nv are visually similar in dermoscopic images, the classifier's decision boundary remains biased toward the still-dominant nv class, illustrating that residual imbalance can affect visually adjacent classes even when their own sample count is not deficient.

For the nv class, the baseline model achieves an F1-score of 0.92 versus 0.85 for the proposed method. This decrease is explained by a fundamentally different classification strategy: the baseline model tends to predict nv for most images, while the proposed method distributes predictions more evenly across classes. Finally, for the vasc class, the proposed method demonstrates the most significant improvement: the F1-score increases from 0.43 to 0.85, and the recall from 0.35 to 0.82, which is due to the increase in the class size in the training set from 113 to 411 samples due to synthetic generation. Figures 4 and 5 show comparison of training curves and confusion matrices for baseline and proposed methods. The baseline model's curve reflects its actual early stopping point (14 epochs) rather than the maximum of 25 epochs allowed by the training configuration. The proposed model's curve spans its full two-phase schedule (5 frozen-backbone epochs followed by 25 fine-tuning epochs, marked by the dashed vertical line), for 30 epochs in total.

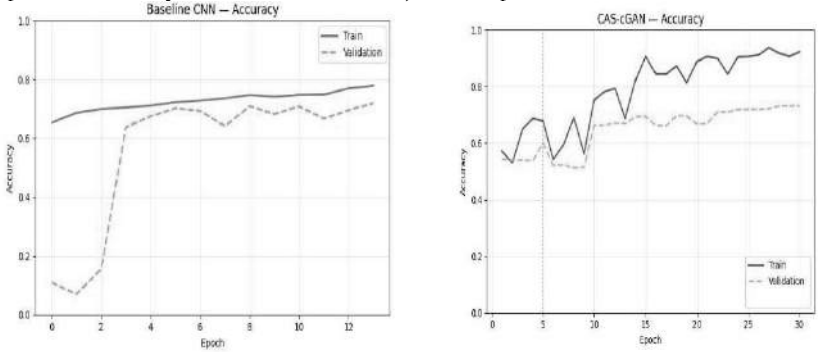


Figure 4. Comparison of the training curves for the baseline method and proposed one.

A comprehensive analysis of the results allows us to formulate several key conclusions. First, standard accuracy as a single evaluation metric is insufficient for classification tasks involving unbalanced medical images: the high accuracy of the baseline model (0.80) masks a complete failure for the df class and critically low recall for mel, akiec, and vasc. The macro-averaged F1-score, on the other hand, accurately reflects performance across all classes – and it is on this metric that the proposed method outperforms the baseline. Secondly, the proposed pipeline addresses a fundamental issue that was not addressed in the baseline implementation:

a systematic bias in the model toward the dominant class. The average recall for the six minority classes in the proposed method is 0.66 versus 0.42 for the baseline model, representing an increase of almost 50% and demonstrating a qualitative shift in the classification strategy – from a focus on the majority to equal recognition of all diagnostic categories.

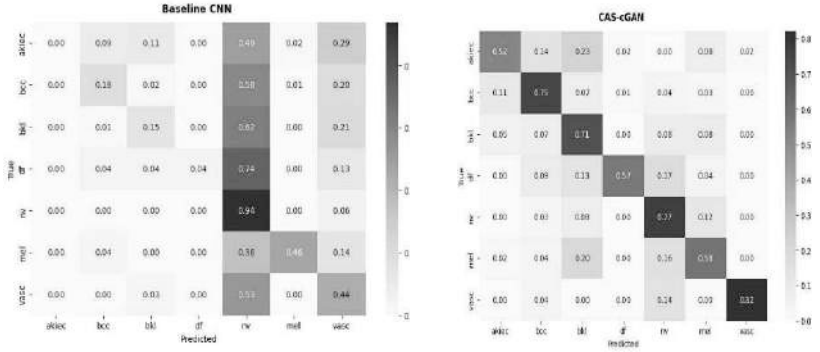


Figure 5. Comparison of the confusion matrices.

Conclusions

This paper addressed the problem of classifying dermatoscopy images under conditions of severe class imbalance – one of the most pressing challenges in the practical application of automated skin lesion diagnostic systems. The proposed Class-Aware Selective cGAN method was developed to address the limitations of existing image balancing approaches, which either fail to reproduce complex visual distributions or include synthetic data in the training set without any quality control.

The main contribution of this paper consists of three interrelated components. The first is the use of a conditional generative adversarial network trained to synthesize class-specific images, which enables targeted enrichment of underrepresented diagnostic categories. The second and most distinctive contribution is the selective filtering mechanism, which evaluates each generated sample against a dual criterion: a confidence threshold and correct attribution to the target class. This mechanism ensures that only high-quality synthetic samples are fed into the training pipeline, preventing the inclusion of noisy or mislabeled examples that could degrade the quality of the final classifier. The third component is an adaptive balancing strategy based on the median class size, which prevents oversaturation of the sample with synthetic data and preserves the natural distribution structure.

Experimental evaluation on the HAM10000 dataset confirmed the effectiveness of the proposed approach. The most significant improvements were recorded for metrics that equally consider all classes: balanced accuracy more than doubled, and the macro-averaged F1-score almost doubled compared to the baseline model. Post-class analysis showed that the improvement covers all minority diagnostic categories without degrading the performance of the dominant class, a fundamentally important result from a clinical perspective. The baseline model completely failed to cope with a number of rare classes, whereas the proposed method achieved significant recognition quality across all seven categories. This confirms the central hypothesis

of the study: targeted synthetic generation with quality control effectively addresses the problem of model bias toward majority classes and fundamentally changes the classification strategy from a focus on the majority to an equal recognition of all diagnostic categories. Prospects for further research cover several areas. First of all, improving the generative component seems the most obvious step: more modern image synthesis architectures, in particular diffusion models, demonstrate fundamentally higher generation quality and training stability compared to classical adversarial networks, and their integration into the proposed pipeline could significantly improve both the sample acceptance rate during filtering and the overall quality of the final classifier. The second promising direction relates to adaptive calibration of the filtering threshold. In the current implementation, the confidence threshold is fixed and uniform for all classes, while its optimal value likely varies significantly depending on the complexity of the visual patterns and the generator's ability to model each specific category.

An adaptive strategy, in which the threshold is determined individually for each class based on the empirical distribution of confidence scores, could improve the balance between filtering rigor and the size of the accepted synthetic samples. An important area is the integration of interpretability methods into the proposed pipeline. In clinical decision support settings, obtaining a correct prognosis is not enough – physician needs to understand which visual features determined a particular classification decision. Incorporating feature significance visualization methods, such as Grad-CAM, would verify that the model is based on clinically relevant patterns rather than artifacts of synthetic data and would be an important step toward the real-world clinical application of the proposed approach.

A separate line of work concerns the evaluator used for filtering. The acceptance rule inherits whatever biases the pre-trained classifier acquired from the real data, so a sample that the evaluator finds convincing is not necessarily one that carries diagnostically meaningful information. An ensemble of independently trained evaluators, or a criterion that combines classifier confidence with a measure of distributional similarity to real images, may therefore yield a more robust decision than a single confidence score obtained from a single model. Closely related is the question of how the components of the pipeline should be tuned together rather than in isolation. The filtering threshold and the target level of class representation were selected independently in this study, yet they interact: a stricter threshold reduces the pool of accepted samples and makes the target level harder to reach, while a more ambitious target forces the acceptance of material the filter would otherwise reject. Treating the two as a single optimisation problem, in which the strictness of selection and the desired degree of balancing are calibrated jointly, appears a more principled approach than fixing each separately. The applicability of the method beyond a single collection also remains to be established. The pipeline makes no assumptions specific to dermatoscopy: conditional generation, quality-aware filtering and median-based planning are independent of one another and of the imaging modality, and each may be replaced without altering the others. This modularity suggests that the approach should transfer to other imbalanced medical benchmarks, and more broadly to recognition tasks in which a small number of categories dominates the available data, but such transfer has yet to be demonstrated empirically.

Finally, the practical value of the approach depends on how it behaves under conditions closer to clinical deployment. Training material accumulates gradually, class proportions shift as new cases arrive, and a model that was balanced at one point may drift out of balance later. An incremental version of the pipeline, in which imbalance is reassessed and generation is repeated as the dataset grows, would allow the balancing strategy to be maintained over time rather than applied once at the moment of training, and would bring the method closer to the requirements of a working diagnostic system.

References

[1] Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., Dehghani, M., Minderer, M., Heigold, G., Gelly, S., Uszkoreit, J., & Houlsby, N. (2021). An image is worth 16x16 words: Transformers for image recognition at scale. International Conference on Learning Representations. https://arxiv.org/abs/2010.11929.

[2] Kim, H. E., Cosa-Linan, A., Santhanam, N., Jannesari, M., Maros, M. E., & Ganslandt, T. (2022). Transfer learning for medical image classification: a literature review. BMC Medical Imaging, 22(1), 69. https://doi.org/10.1186/s12880-022-00793-7.

[3] Yu, X., Wang, J., Hong, Q.-Q., Teku, R., Wang, S.-H., & Zhang, Y.-D. (2022). Transfer learning for medical images analyses: A survey. Neurocomputing, 489, 230–254. https://doi.org/10.1016/j.neucom.2021.10.121.

[4] Rezvani, S., & Wang, X. (2023). A broad review on class imbalance learning techniques. Applied Soft Computing, 143, 110415. https://doi.org/10.1016/j.asoc.2023.110415.

[5] Gui, Q., Zhou, H., Guo, N., & Niu, B. (2023). A survey of class-imbalanced semi-supervised learning. Machine Learning, 113, 5057–5086. https://doi.org/10.1007/s10994-023-06344-7.

[6] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. Journal of Artificial Intelligence Research, 16, 321–357. https://doi.org/10.1613/jair.953.

[7] Sharma, A., Singh, P. K., & Chandra, R. (2022). SMOTified-GAN for class imbalanced pattern classification problems. IEEE Access, 10, 30655–30665. https://doi.org/10.1109/ACCESS.2022.3158977.

[8] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems, 27. https://doi.org/10.1145/3422622.

[9] Mirza, M., & Osindero, S. (2014). Conditional generative adversarial nets. arXiv preprint. https://doi.org/10.48550/arXiv.1411.1784.

[10] Liu, A., Ghosh, J., & Martin, C. (2021). A survey on generative adversarial networks for imbalance problems in computer vision tasks. Journal of Big Data, 8(1), 27. https://doi.org/10.1186/s40537-021-00414-0.

[11] Yadav, P., Sihag, G., & Vijay, V. (2025). Rebalancing the scales: A systematic mapping study of generative adversarial networks (GANs) in addressing data imbalance. arXiv preprint. https://arxiv.org/abs/2502.16535.

[12] Hou, B., & Chen, G. (2024). A new imbalanced data oversampling method based on Bootstrap method and Wasserstein Generative Adversarial Network. Mathematical Biosciences and Engineering, 21(3). https://doi.org/10.3934/mbe.2024190.

[13] Gökcen, A., & Boyacı, A. (2025). Robust federated learning with confidence-weighted filtering and GAN-based completion under noisy and incomplete data. arXiv preprint. https://arxiv.org/abs/2505.09733.

[14] Azizi, S., Kornblith, S., Saharia, C., Norouzi, M., & Fleet, D. J. (2023). Synthetic data from diffusion models improves ImageNet classification. arXiv preprint. https://doi.org/10.48550/arXiv.2304.08466.

[15] Sagers, L. W., et al. (2023). Augmenting medical image classifiers with synthetic data from latent diffusion models. arXiv preprint. https://arxiv.org/abs/2308.12453.
[16] Akrout, M., et al. (2023). Diffusion-based data augmentation for skin disease classification: Impact across original medical datasets to fully synthetic images. Deep Generative Models (MICCAI Workshop), Lecture Notes in Computer Science, 14533, 99–109. https://doi.org/10.1007/978-3-031-53767-7_10.
[17] Nguyen, V. D., Bui, N. D., & Do, H. K. (2022). Skin lesion classification on imbalanced data using deep learning with soft attention. Sensors, 22(19), 7530. https://doi.org/10.3390/s22197530.
[18] Shetty, B., Fernandes, R., Rodrigues, A. P., Chengoden, R., Bhattacharya, S., & Lakshmanna, K. (2022). Skin lesion classification of dermoscopic images using machine learning and convolutional neural network. Scientific Reports, 12(1), 18134. https://doi.org/10.1038/s41598-022-22644-9.
[19] Kishanthan, S., & Hevapathige, A. (2025). Deep learning meets oversampling: A learning framework to handle imbalanced classification. International Journal of Information Technology, 17, 4491–4503 (2025). https://doi.org/10.1007/s41870-025-02690-y.
[20] Mendeley Data. (2025). Balanced and augmented version of the HAM10000 skin lesion dataset (derived & corrected). https://data.mendeley.com/datasets/hpcf9psdy7/1.
[21] Tschandl, P., Rosendahl, C., & Kittler, H. "The HAM10000 Dataset: A Large Collection of Multi-Source Dermatoscopic Images of Common Pigmented Skin Lesions". Scientific Data. 2018; 5: 180161. https://doi.org/10.1038/sdata.2018.161.
[22] Skin Cancer: HAM10000 baseline notebook: https://www.kaggle.com/code/ mittshah/ skin-cancer-ham10000/notebook.

УМОВНІ ГЕНЕРАТИВНІ МОДЕЛІ З КОНТРОЛЕМ ЯКОСТІ СИНТЕТИЧНИХ ДАНИХ ДЛЯ РОЗПІЗНАВАННЯ НЕДОСТАТНЬО ПРЕДСТАВЛЕНИХ КАТЕГОРІЙ МЕДИЧНИХ ЗОБРАЖЕНЬ

Міхалев К., Ph.D., Ніколенко А.
Національний університет «Одеська політехніка», Україна

Анотація. *У цій статті розглядається проблема дисбалансу класів, яка є одним із ключових обмежень у побудові систем розпізнавання зображень у задачах комп'ютерного зору. Дисбаланс між класами, в якому деякі діагностичні категорії представлені тисячами зразків, а інші містять лише кілька десятків, призводить до систематичного зміщення моделей у бік домінантних класів та повної неможливості розпізнавати рідкісні патології, що є неприйнятним у клінічному контексті. У статті розглядаються методи генерації синтетичних даних на основі умовних генеративно-змагальних мереж, механізми вибіркової фільтрації синтетичних зразків, а також стратегії адаптивного балансування зразків з використанням медіанного цільового рівня представленості класів. Особлива увага приділяється механізму вибіркової фільтрації як ключовому науковому внеску роботи, що відрізняє запропонований підхід від існуючих методів балансування на основі генеративних моделей. Результати демонструють, що запропонований метод забезпечує значне покращення збалансованої точності та макроусередненого F1-балу порівняно з базовою моделлю. Крім того, дослідження показує, що поєднання умовної генерації зображень з двокритеріальною фільтрацією синтетичних зразків дозволяє досягти значного рівня розпізнавання для всіх класів меншин.*

Ключові слова: *незбалансованість класів, генеративно-змагальні мережі, генерація зображень, селективна фільтрація, розпізнавання зображень*

УДК 004.8:004.93:624.04(477)
DOI

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВІЗУАЛЬНО-МОВНИХ МОДЕЛЕЙ ДЛЯ КЛАСИФІКАЦІЇ ПОШКОДЖЕНЬ ІНФРАСТРУКТУРИ: НА ПРИКЛАДІ УКРАЇНИ

Ph.D., Іванов О.[1][0000-0002-8620-974X], Бєляєв К.[2][0009-0001-7135-3562], Олійник В.[3][0009-0000-5527-7750], Арсірій О.[4][0000-0001-8660-6916]
[1,2,3]Національний університет «Одеська політехніка», Україна,
[4]Одеський національний морський університет, Україна
EMAIL: [1]lesha.ivanoff@gmail.com, [2]kirillbelyaev2921@gmail.com,
[3]vadimol081@gmail.com, [4]elena.arsiriy@gmail.com

Анотація. *Масштабне руйнування цивільної інфраструктури, спричинене війною в Україні, зумовило нагальну потребу в автоматизованих, надійних та масштабованих методах оцінювання структурних пошкоджень. У цьому дослідженні представлено порівняльну оцінку сучасних візуально-мовних моделей (ВММ) та гібридного підходу на основі комп'ютерного зору для класифікації пошкоджень інфраструктури за кількома ракурсами. Спеціалізований набір даних був сформований на основі наземних зображень пошкоджених війною будівель, зібраних у різних регіонах України, де кожен об'єкт інфраструктури представлений від двох до восьми фотографій, включно з ракурсами до та після пошкодження, якщо вони були доступні. Ступінь тяжкості пошкоджень класифіковано за п'ятьма категоріями: від неушкодженого до повністю зруйнованого. Запропонована методологія інтегрує систему багатовидового аналізу з семантичною сегментацією на основі архітектури U-Net із застосуванням кодувальника ResNet та евристичної моделі, заснованої на правилах, яка оцінює структурні пошкодження з використанням піксельних метрик. Дані, отримані з кількох ракурсів, агрегуються для формування єдиної оцінки стану об'єкта, що зменшує двозначність, спричинену перекриттям або обмеженими кутами огляду. Запропонований підхід був експериментально порівняний із кількома вдосконаленими мультимодальними ВММ, включаючи GPT-5.5, Claude Sonnet 5, Gemini 3.1 Pro та Grok 4, за такими показниками, як Точність (Accuracy), Прецизійність (Precision), Повнота (Recall), F1-показник та коефіцієнти переоцінки/недооцінки. Експериментальне оцінювання, проведене на спеціалізованому наборі даних зі 108 об'єктів інфраструктури, демонструє, що вдосконалені ВММ перевершують базову модель сегментації за загальною точністю класифікації, забезпечуючи надійний аналіз складних сценаріїв структурних пошкоджень. Водночас запропонована гібридна структура на основі сегментації пропонує інтерпретовану оцінку пошкоджень на рівні пікселів і залишається придатною для розгортання в умовах обмежених ресурсів. Розроблена методологія багатовидової оцінки стане ключовим аналітичним компонентом інтелектуальної багатофункціональної ГІС, призначеної для підтримки обліку будівельних та демонтажних відходів (БДВ), оптимізації логістики перероблення та сприяння сталому післявоєнному відновленню на основі принципів циркулярної економіки.*

Ключові слова. *Оцінка пошкоджень інфраструктури, візуально-мовні моделі, багатовидовий аналіз зображень, семантична сегментація, будівельні та демонтажні відходи, штучний інтелект.*

1. Вступ

Масштаби руйнувань інфраструктури, спричинені війною в Україні, призвели до утворення безпрецедентних обсягів будівельних та демонтажних відходів (БДВ), що вимагає швидких, автоматизованих систем обліку для заміни повільних та небезпечних ручних оцінок. У цій роботі представлено інтелектуальну систему аналізу зображень, розроблену як ключовий компонент інтелектуальної багатофункціональної ГІС для обліку БДВ.

Для навчання та валідації системи нами було сформовано рідкісний, високоспеціалізований набір даних, що включає багатовидові зображення (від 2 до 8 ракурсів на об’єкт, включно зі станами «до» та «після») пошкоджених війною об'єктів інфраструктури по всій території України. Об'єкти класифіковано за п’ятьма чіткими рівнями пошкоджень (0 – Неушкоджений до 4 – Зруйнований) на основі послідовних візуальних критеріїв. Ми пропонуємо гібридний метод класифікації, який інтегрує глибоке вилучення ознак за допомогою архітектури U-Net з кодувальником ResNet та евристичною моделлю, заснованою на правилах. Ця евристична модель оцінює співвідношення пошкоджень у пікселях для трьох ключових регіонів інтересу: покрівля, структурна цілісність/фасад та засклення. Продуктивність цього гібридного підходу U-Net-ResNet-евристика порівнюється з сучасними візуально-мовними моделями (ВММ) з використанням стратегії багатовидової агрегації, яка визначає загальний стан об'єкта на основі максимального видимого пошкодження. Оцінювання проводиться за стандартними метриками: Точність (Accuracy), Прецизійність (Precision), Повнота (Recall), F1-показник та коефіцієнт переоцінки/недооцінки. Результати демонструють, що поєднання глибокого навчання сегментації з евристикою на основі правил забезпечує високоінтерпретовані та точні класифікації. Цей автоматизований конвеєр оцінки пошкоджень слугує критично важливою основою для інтелектуальної багатофункціональної ГІС-платформи, що уможливлює оптимізовану логістику перероблення БДВ та підтримує принципи циркулярної економіки під час сталого відновлення України.

2. Аналіз попередніх досліджень

Інтеграція штучного інтелекту (ШІ), комп’ютерного зору та геопросторових технологій нещодавно стала ключовою сферою у сталому будівництві та відновленні після стихійних лих. Цей розділ оглядає наявні методології оцінки пошкоджень будівель та управління БДВ, структурувавши їх за трьома основними напрямами.

Глибоке навчання в оцінці наслідків стихійних лих та класифікації БДВ. Традиційні методи управління будівельними відходами та відходами від знесення значною мірою покладалися на ручні інспекції, які є невід’ємно повільними, трудомісткими та схильними до людських помилок. Для подолання цих обмежень дослідники все частіше звертаються до машинного навчання. Ґрунтовну базу для таких підходів забезпечує робота Samal та ін. [1], у якій представлено критичний огляд різноманітних методів машинного навчання, що застосовуються для оцінювання, класифікації та прогнозування обсягів БДВ, підкреслюючи їхню роль у забезпеченні сталого управління відходами. У масштабах супутникового дистанційного зондування знаковою

роботою стала праця Gupta та ін. [2], яка представила набір даних xBD, що залишається «золотим стандартом» у виявленні змін та оцінці пошкоджень будівель. Надаючи багатоканальні супутникові знімки до та після подій із понад 700 000 полігонів будівель та порядковими мітками пошкоджень у 15 країнах, xBD продемонстрував життєздатність пасивного великомасштабного дистанційного зондування для прискорення відновлення після катастроф та зниження ризиків для служб першого реагування. У роботі [3] автор запропонував двоетапний конвеєр машинного навчання для автоматизованої оцінки пошкоджень, що поєднує семантичну сегментацію для виявлення будівель із моделями класифікації та регресії для оцінки тяжкості. Навчаючись на наборі даних xBD та проводячи донавчання (fine-tuning) на власних даних з України, дослідження демонструє ефективне, адаптивне рішення для швидкого моніторингу інфраструктури в умовах післявоєнних міських середовищ. Спираючись на ці прогнозні моделі, комп'ютерний зір було застосовано для класифікації відходів безпосередньо з візуальних даних. Наприклад, Molchanova та ін. [4] запропонували спеціалізований метод класифікації БДВ з використанням двофакторного нейромережевого аналізу зображень. Використовуючи стійкі архітектури згорткових нейронних мереж (CNN), такі як YOLO та ResNet, їхній підхід демонструє, як глибоке навчання може автоматизувати ідентифікацію різних категорій відходів на знімках об'єктів, закладаючи основу для автоматизованих конвеєрів сортування та перероблення. Guo та ін. [5] представили новий фреймворк сегментації тріщин із нульовим навчанням (zero-shot) для моніторингу структурної цілісності цивільної інфраструктури, який використовує супервізію на рівні зображень та модель Segment Anything, щоб усунути потребу в трудомісткій ручній анотації на рівні пікселів. Zheng та ін. [6] впровадили ChangeOS – фреймворк семантичного виявлення змін на основі об'єктів, що інтегрує локалізацію об'єктів із класифікацією пошкоджень для покращення оцінки пошкоджень будівель за допомогою двочасових супутникових знімків. Поєднуючи потужне представлення ознак глибокого навчання з семантичною узгодженістю об'єктного аналізу, запропонована модель «end-to-end» досягає вищої точності та узагальнення при картуванні пошкоджень як від стихійних лих, так і від техногенних вибухів. Duarte та ін. [7] запропонували три підходи до злиття ознак CNN з мультироздільною здатністю для покращення оцінки пошкоджень будівель шляхом інтеграції знімків з різних просторових платформ, таких як супутникові та аерофотознімки. Дослідження демонструє, що злиття карт ознак з проміжних шарів мережі покращує як точність класифікації, так і можливості локалізації, пропонуючи більш надійну альтернативу традиційним монороздільним методам аналізу після катастроф.

Перспективні ВММ та генеративний ШІ для візуальної діагностики. Хоча традиційні CNN відмінно справляються з вузькими завданнями класифікації та сегментації, стрімка еволюція ВММ відкрила нові парадигми. Генеративний ШІ та ВММ пропонують багатообіцяючі можливості через розуміння контексту зображень за допомогою запитів на природній мові та токенізації. Estêvão [8] оцінив ефективність моделей генеративного ШІ для оцінки пошкоджень після землетрусів, підкресливши, як ці передові системи можуть токенізувати

структурні особливості для ідентифікації рівнів пошкоджень та класифікації типів матеріалів з мінімальним навчанням під конкретне завдання. Ширший потенціал цих інтелектуальних систем досліджується Alimi та ін. [9]. У їхньому огляді літератури розглядається, як ШІ, машинне навчання та обробка природної мови можуть бути поєднані для оптимізації робочих процесів управління БДВ, прогнозування темпів утворення відходів та активного виявлення можливостей для циркулярного повторного використання та перероблення матеріалів. Перехід до таких мультимодальних ШІ-систем дозволяє створювати більш інтерпретовані та гнучкі діагностичні інструменти у структурній інженерії.

Оцінка руйнувань, спричинених війною, та виклики циркулярної економіки. Візуальні патерни пошкоджень, спричинені військовими конфліктами, значно відрізняються від тих, що спричинені природними катастрофами, такими як землетруси чи урагани. Військові пошкодження характеризуються локалізованими балістичними впливами, інтенсивним фрагментуванням, подрібненням бетону та змішаним сміттям. У дослідженні [10] запропоновано комплексну стратегію управління будівельними відходами, що виникають внаслідок бойових дій в Україні, з акцентом на впровадженні принципів циркулярної економіки та створенні ринку вторинних матеріалів. Розглядаючи цей специфічний виклик у контексті війни в Україні, дуже актуальний проєкт, описаний Aouf [11], демонструє, як крайовий (edge-based) ШІ може аналізувати кадри з дронів, зняті над зруйнованими будівлями. Ця система успішно ідентифікує придатні для повторного використання матеріали серед уламків, активно сприяючи «циркулярності на місці» під час невідкладних зусиль з відновлення. Aimaiti та ін. [12] оцінили ефективність середньороздільних супутникових знімків Sentinel-1 (SAR) та Sentinel-2 (оптичних) для швидкої оцінки пошкоджень будівель у Київській області під час поточної війни. Поєднуючи виявлення змін інтенсивності та аналіз текстур із маскуванням забудованих територій, автори демонструють, що супутникові дані з відкритим доступом забезпечують надійний, масштабований метод початкового картування пошкоджень там, де наземна верифікація обмежена. Для фіксації критичних структурних деталей, які залишаються невидимими на супутникових знімках, наземна оцінка пошкоджень будівель стала надзвичайно актуальною. Вагомий внесок у цю нішу зробили Lysanets та ін. [13], які запропонували фреймворк U-Net з розширеними ембеддингами (embedding-enhanced), використовуючи підхід на основі патчів, та представили перший набір даних пошкоджень під час війни для сегментації будівель на рівні землі. Їхня робота орієнтована на зображення збоку пошкоджених українських будівель з піксельною анотацією за шістьма класами (включаючи «Пошкоджений дах» та «Розбите вікно»). Інтегрувавши глобальні ембеддинги ConvNeXt-Large у класичний енкодер U-Net, вони досягли значного підвищення продуктивності (досягнувши F1-показника 0,8982 з архітектурою ResNet-50), підтвердивши ефективність поєднання глибокого навчання на основі U-Net з передовим вилученням ознак для комплексних завдань структурних пошкоджень у реальних умовах.

Це дослідження базується на концептуальному фреймворку, запропонованому у нашій попередній роботі [14], яка представила інтелектуальну інформаційну технологію для управління БДВ. Тодішнє дослідження заклало фундаментальну базу знань ГІС, що інтегрує просторові та атрибутивні дані для системи картування «Джерела-Пункти прийому», використовуючи ВММ для інтерпретації візуальних ознак та оптимізації транспортних маршрутів для вторинних ресурсів. Попри ці досягнення, залишається критичний пробіл у знаннях: більшість існуючих наборів даних з відкритим кодом (як-от xBD) зосереджені на природних катастрофах. Існує нагальна потреба у багатовидових наборах даних високої роздільної здатності, що відображають фактичні воєнні структурні пошкодження для валідації та вдосконалення ШІ-моделей для розгортання в зонах конфліктів.

3. Постановка мети дослідження

Метою цього дослідження є розробка та експериментальне оцінювання методу автоматизованої класифікації тяжкості пошкоджень інфраструктури на основі аналізу зображень із багатьох ракурсів з використанням сучасних ВММ. Для досягнення цієї мети вирішуються такі завдання:

– створення та підготовка спеціалізованого набору даних українських інфраструктурних об’єктів, представлених багатовидовими наборами зображень (від 2 до 8 фотографій на об’єкт);

– розробка логічного фреймворку для технології інтелектуальної багатовидової класифікації, що включає підготовку даних, контекстний аналіз зображень за допомогою мультимодальної моделі, агрегацію результатів та валідацію отриманих прогнозів;

– впровадження методу оцінки пошкоджень з кількох ракурсів, який поєднує аналіз зображень, виконаний візуально-мовними моделями, з піксельними характеристиками пошкоджених структурних компонентів та алгоритмом інтеграції результатів з багатьох точок огляду;

– проведення порівняльного експериментального оцінювання сучасних візуально-мовних моделей для класифікації пошкоджень інфраструктури з використанням метрик Accuracy (Точність), Precision (Прецизійність), Recall (Повнота) та F1-score (F1-показник), а також оцінка схильності моделей до переоцінки або недооцінки тяжкості пошкоджень.

4. Методологія

4.1 Робочий процес оцінки пошкоджень на основі ШІ

Запропонована методологія розроблена для автоматичної оцінки пошкоджень об’єктів цивільної інфраструктури з використанням мультимодального штучного інтелекту. На відміну від звичайних підходів до класифікації зображень, де кожне зображення обробляється незалежно, запропонований робочий процес розглядає інфраструктурний об’єкт як єдину аналітичну сутність, представлену кількома фотографіями, знятими з різних точок огляду. Ця багаторакурсна стратегія знижує ймовірність помилкової оцінки, спричиненої частковою видимістю структурних пошкоджень, і дозволяє отримати більш надійну класифікацію загального стану об’єкта.

Загальна блок-схема робочого процесу інтелектуальної системи оцінки пошкоджень будівель проілюстрована на рис. 1.

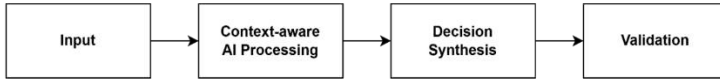


Рисунок 1. Блок-схема робочого процесу оцінки пошкоджень будівель на основі ШІ

Першим етапом робочого процесу є введення даних. Вхідні дані системи складаються з пакета фотографій, що представляють один і той самий інфраструктурний об'єкт. Кожен об'єкт описується набором з N зображень, зроблених з різних точок огляду. Пакет зображень має включати фотографії, зроблені до та після пошкодження, що дозволяє моделі порівнювати структурні зміни з часом.

Другим етапом є контекстно-залежна обробка ШІ. Замість аналізу кожного зображення окремо, повний пакет фотографій одночасно надається мультимодальній ВММ разом із специфічним запитом (промптом). Запит інструктує модель спільно проаналізувати всі доступні ракурси та визначити найвищий рівень структурних пошкоджень. Враховуючи просторову узгодженість між ракурсами, модель може виявити пошкодження, які можуть бути невидимі з одного кута камери.

Третім етапом є синтез рішень. Мультимодальна модель агрегує візуальні докази, вилучені з усіх ракурсів, і видає єдину мітку пошкодження, що представляє загальний стан інфраструктурного об'єкта. Цей процес відповідає принципам багатовидової класифікації, де остаточний прогноз генерується на рівні об'єкта, а не на рівні окремого зображення.

Останнім етапом робочого процесу є валідація результатів. Прогнозований клас пошкодження порівнюється з еталонною анотацією (ground truth), присвоєною людиною-анотатором. Продуктивність моделі оцінюється за допомогою стандартних метрик класифікації, включаючи Accuracy, Precision, Recall та F1-score.

4.2 Агрегація даних та підготовка набору даних

Запропонована методологія розглядає інфраструктурний об'єкт, а не окреме зображення, як основну одиницю аналізу. Кожен об'єкт представлений колекцією фотографій, знятих з багатьох точок огляду, що дозволяє комплексно оцінити структурні пошкодження. Це представлення відповідає принципам багатовидової класифікації зображень, де остаточний прогноз присвоюється об'єкту після спільного аналізу всіх доступних візуальних спостережень. Формально кожен інфраструктурний об'єкт представлений як:

$$O_i = \{I_1, I_2, ..., I_j, ..., I_k\}, k \geq 2, \quad (1)$$

де O_i позначає *i*-й інфраструктурний об'єкт, I_j представляє окреме зображення, зняте з певної точки огляду, а k – кількість доступних ракурсів.

Якщо доступно, набір зображень може містити фотографії, зроблені як до, так і після події пошкодження. У цьому випадку представлення об'єкта можна виразити як:

$$O_i = \{I_1^{before}, ..., I_m^{before}, I_1^{after}, ..., I_n^{after}\}, \quad (2)$$

де $m+n=k$. Зображення «до» надають довідкову інформацію про початковий вигляд споруди, тоді як зображення «після» містять докази можливих

пошкоджень. Якщо довідкові зображення відсутні, оцінка виконується виключно з використанням спостережень після події.

На відміну від звичайних наборів даних класифікації зображень, де кожне зображення є незалежною вибіркою, запропонований набір даних організовує зображення у групи на рівні об'єкта. Отже, кожен прогноз відповідає цілому інфраструктурному об'єкту, а не окремій фотографії. Такий дизайн суттєво зменшує неоднозначність, спричинену перекриттями, обмеженими кутами огляду або локально невидимими структурними дефектами, і забезпечує більш надійну оцінку фактичного рівня пошкодження.

4.3 Схема класифікації даних

Для забезпечення послідовної анотації та оцінювання всі інфраструктурні об'єкти розподіляються до одного з п'яти взаємовиключних класів пошкоджень. Запропонована класифікація дотримується прогресивної шкали від неушкоджених споруд до повного руйнування і базується виключно на видимих структурних характеристиках, що спостерігаються з усіх доступних ракурсів. Під час анотування остаточний клас визначається відповідно до найвищого рівня пошкодження, видимого на будь-якому зображенні, що належить до об'єкта.

Клас 0 – Неушкоджений. Будівля візуально ціла, без видимих структурних дефектів. На фасаді немає тріщин, дах неушкоджений, віконне скління ціле, загальна геометрія будівлі збережена.

Клас 1 – Незначні пошкодження. Спостерігаються незначні поверхневі пошкодження, тоді як структурна цілісність залишається незмінною. Типовими ознаками є розбите віконне скло при цілих рамах, невеликі дефекти фасаду, такі як сколи штукатурки або сліди від осколків, та обмежені пошкодження покрівлі без наскрізних отворів чи структурних деформацій.

Клас 2 – Помірні пошкодження. Будівля демонструє локалізовані структурні пошкодження, але залишається стабільною. Видимими ознаками є наскрізні отвори у зовнішніх стінах або даху, повна втрата віконних чи балконних блоків та локалізовані пошкодження структурних елементів. Основний несучий каркас та загальна геометрія будівлі залишаються збереженими, без обвалення цілих кімнат чи поверхів.

Клас 3 – Значні пошкодження. Наявне суттєве порушення структурної цілісності. Характеристиками, що спостерігаються, є часткове обвалення стін, відкриття внутрішніх приміщень, обвалення плит перекриття, виражена деформація конструктивного каркаса та значна втрата ділянок даху. Хоча частини будівлі залишаються стояти, її структурна стабільність критично порушена.

Клас 4 – Зруйнований. Початкова геометрія будівлі більше не впізнавана. Конструкція обвалилася в руїни, залишилися лише фрагменти нижніх стін, ізольовані структурні залишки або фундамент. Об'єкт вважається повністю зруйнованим і більше не придатним до експлуатації.

4.4 Стратегія мультизображувального промптингу

На відміну від звичайних класифікаторів глибокого навчання, які обробляють окремі зображення незалежно, ВММ дозволяють проводити одночасне міркування над кількома зображеннями у спільному розмовному

контексті. У запропонованій методології всі фотографії, що відповідають одному інфраструктурному об'єкту, подаються моделі в одному запиті. Це дозволяє моделі агрегувати візуальні докази з різних ракурсів і видати єдину оцінку на рівні об'єкта. Запит інструктує модель виконувати роль незалежного експерта зі структурної інспекції та оцінки пошкоджень після катастроф і оцінювати лише видимі докази, присутні на наданих фотографіях. Оцінка чітко виключає припущення щодо прихованих структурних елементів або причини пошкодження. Крім того, моделі доручено спільно розглядати всі доступні зображення та призначити один остаточний клас пошкодження, що відповідає загальному стану об'єкта. Запит, використаний у цьому дослідженні, наведено нижче.

«*Ви дієте як незалежний експерт зі структурної інспекції та оцінки пошкоджень будівель і цивільної інфраструктури після катастроф. Ваше завдання – виконати об'єктивну візуальну оцінку одного інфраструктурного об'єкта з використанням наданих фотографій, отриманих до та після події пошкодження, і визначити його загальний клас пошкодження. Кожен об'єкт може містити одну або кілька фотографій, що відображають як умови до події, так і після неї. Усі фотографії, що належать до одного об'єкта, повинні бути проаналізовані спільно як єдине джерело інформації, і має бути призначено лише один остаточний клас пошкодження. Оцінюйте лише інформацію, безпосередньо видиму на зображеннях. Не робіть припущень щодо структурних елементів, які не є видимими, і не робіть висновків про причину пошкодження. Оцінюйте будівлю як інтегровану конструкцію. Жодна окрема візуальна ознака не повинна визначати клас пошкодження сама по собі. Наприклад, розбиті вікна або значні пошкодження фасаду самі по собі не вказують на серйозні структурні пошкодження. Основними критеріями оцінки є стан несучої конструкції, збереження геометрії будівлі та загальна структурна цілісність. Класифікуйте об'єкт відповідно до наступної шкали...*» (Далі наведено опис класів 0–4).

Структурований запит стандартизує процес мислення мультимодальної моделі та гарантує, що кожен інфраструктурний об'єкт оцінюється за ідентичними критеріями. Чітко інструктуючи модель агрегувати докази з багатьох ракурсів і зосереджуватися на структурній цілісності, а не на ізольованих візуальних дефектах, запропонована стратегія запитів зменшує неоднозначність та покращує узгодженість класифікації пошкоджень на рівні об'єкта. Крім того, структурований текстовий вивід полегшує подальше порівняння з вручну анотованими мітками «ground truth» та дозволяє безпосередньо обчислювати метрики оцінювання.

5. Пропонований метод оцінки пошкоджень на основі багатовидового сегментаційного аналізу та піксельних метрик

Для семантичної сегментації пошкоджень будівель за наземними знімками ми використовуємо глибоку згорткову нейронну мережу, що поєднує симетричний декодер U-Net із попередньо навченим енкодером ResNet-34. Пропускні зв'язки (skip connections) безпосередньо передають високочастотні просторові ознаки – такі як структурні тріщини та уламки скла – з ранніх етапів енкодера до декодера, запобігаючи втратам просторової дискретизації під час зменшення роздільної здатності. Модель навчена на спеціальному наборі даних воєнних пошкоджень [13, 15], що містить 290 зображень високої роздільної здатності з видом збоку пошкоджених будівель в Україні. Піксельні анотації охоплюють шість семантичних класів: Інше (клас 0, 66,10 % пікселів), Будівля

(клас 1, 19,42 %), Дах (клас 2), Пошкодження (клас 3), Розбите вікно (клас 4, 2,66 %) та Пошкоджений дах (клас 5, 1,92 %). Щоб зберегти дрібні текстури, зображення сегментуються за допомогою змінного вікна на патчі 640 × 640 пікселів із кроком 160. Логіти патчів, що перекриваються, усереднюються перед застосуванням функції Softmax для усунення крайових артефактів. Критичним обмеженням цього набору даних є те, що анотації обмежені суворо «пост-пошкодженими» зображеннями. Не маючи опорної геометрії «до пошкодження», стандартні моделі демонструють високе зміщення класифікації (classification bias) і схильні до недооцінки фактичної структурної деградації. Основним внеском цього дослідження є фреймворк математичної інтерпретації, розроблений для усунення цього зміщення. Застосовуючи оптимізоване мікропорогове значення та зважену агрегацію балів з багатьох ракурсів, фреймворк перетворює необроблені маски сегментації на надійні, безпечно обмежені класи структурної цілісності.

Шість базових класів агрегуються у три чіткі Регіони інтересу (regions of interest, ROI) для вилучення фізичних метрик площі. Площа будівлі (P_{building}): загальна кількість пікселів, що представляють активні структури:

$$P_{building} = \sum pixels(mask \in [1,2,3,4,5]) \quad (3)$$

Площа структурних пошкоджень ($P_{\text{structural_damage}}$): комбіновані пікселі пошкоджених стін та дахів, що загрожують несучій здатності:

$$P_{structural_damage} = \sum pixels(mask \in [3,5]) \quad (4)$$

Площа пошкодження вікон ($P_{\text{window_damage}}$): пікселі, що представляють пошкоджені елементи скління:

$$P_{window_damage} = \sum pixels(mask == 4) \quad (5)$$

Ці сегментовані масиви пікселів формують вхідні дані для конвеєра прийняття рішень. Якісна продуктивність модифікованої моделі U-Net у виділенні цільових структурних та пошкоджених меж показана на рис. 2.



Рисунок 2. Візуалізація моделі сегментації: вхідне зображення фасаду в парі з накладеними кольоровими масками ROI

Щоб усунути дисперсію масштабу, спричинену відстанями зйомки, площі перетворюються на нормалізовані коефіцієнти. Коефіцієнт структурних пошкоджень (R_{str}) та коефіцієнт пошкодження скління (R_{w}) обчислюються відносно загального видимого силуету будівлі:

$$R_{str} = \left(\frac{P_{structural_damage}}{P_{building}} \right) \times 100\% \quad (6)$$

$$R_{str} = \left(\frac{P_{window_damage}}{P_{building}} \right) \times 100\% \quad (7)$$

Для протидії зміщенню моделі через обмеження навчання на даних «після пошкодження» ми впроваджуємо нелінійне дерево рішень експерта:

$$= \begin{cases} 4, \ if \quad R_{str} > 70\% \\ 3, \ if \quad 35\% < R_{str} \le 70\% \\ 2, \ if \quad 14\% < R_{str} \le 35\% \vee (R_{str} \le 6\% \wedge R_w > 20\%) \\ 1, \ if \quad 6\% < R_{str} \le 14\% \vee (R_{str} \le 6\% \wedge R_w \le 20\% \wedge (R_w > 6\% \vee R_{str} > 2\%) \\ 0 \quad else \end{cases} \quad (8)$$

Пороги калібруються відповідно до емпіричних інженерних стандартів на жорстких структурних інтервалах (6,0% – 14,0% – 35,0% – 70,0%).

Наземне оцінювання з використанням одного ракурсу схильне до помилок оклюзії (наприклад, цілий передній фасад маскує обвалену задню стіну). Для багатовидових наборів ($2 \le N \le 8$) ми впроваджуємо двофакторний конвеєр агрегації. Для кожного окремого ракурсу обчислюється лінійний необроблений бал шляхом масштабування структурних та скляних компонентів з локалізованими інженерними вагами:

$$Score^{(i)} = 1.0 \times R_{str}^{(i)} + 0.2 \times R_w^{(i)} \quad (9)$$

Щоб збалансувати локалізовані, серйозні пошкодження із загальним станом усього активу, формулюється глобальний бал (S_{object}) як опукла комбінація максимальних та середніх перспективних балів:

$$S_{object} = \alpha \times \max_{i=1...N}(Score^{(i)}) + (1-\alpha) \times Mean(Score^{(i)}) \quad (10)$$

де $\alpha = 0{,}35$ – математично оптимізована вага.

Остаточний структурний клас будівлі ($Class_{final}$) визначається за допомогою відкаліброваних меж прийняття рішень (T_1= 6,0;T_2= 17,0; T_3= 25,0):

$$Class_{final} = \begin{cases} 4, \ if \quad S_{object} > 70\% \\ 3, \ if \quad T_3 < S_{object} в \%\% \le 70\% \\ 2, \ if \quad T_2 < S_{object} в \%\% \le T_3 \\ 1, \ if \quad T_1 < S_{object} в \%\% \le T_2 \\ 0 \ \ if \quad S_{object} в \%\% \le T_1 \end{cases} \quad (11)$$

Параметр α та пороги прийняття рішень визначено за допомогою протоколу емпіричної оптимізації методом сіткового пошуку (Grid Search) у заданому просторі параметрів ($\alpha \in [0{,}35; 0{,}50]$ із кроком 0,05; T_1, T_2, $T_3 \in [1; 100]$ із кроками 1,0 та 2,0). Цільова функція була спрямована на максимізацію

загальної точності багатокласової класифікації (Accuracy) та метрики Macro-F1 на всьому наборі даних. Ця процедура калібрування гарантує оптимальний баланс між пріоритезацією локальних важких пошкоджень та придушенням ізольованого піксельного шуму сегментації. Ця двофакторна модель забезпечує дотримання безпекового обмеження. Якщо серйозна відмова зафіксована навіть на одній перспективі, максимальний член через λ витягує глобальний бал у відповідний клас небезпеки. Одночасно середній член пригнічує шум від ізольованих аномалій сегментації, забезпечуючи надійність перед передачею даних до ГІС-картування та мереж маршрутизації циркулярної економіки для будівельних відходів.

6. Експерименти та результати

Для оцінки ефективності запропонованого фреймворку інтерпретації та багатовидової агрегації ми зібрали та анотували спеціальний регіональний тестовий набір даних. Набір даних складається з пошкоджених об'єктів цивільної інфраструктури, що постраждали від військових ударів у різних адміністративних регіонах України. Для кожної фізичної будівлі ми розробили структурований запис у базі даних для фіксації як просторових атрибутів, так і візуальних пар. Зібрані схеми метаданих спрощені до трьох функціональних категорій:

– просторові метадані та метадані класифікації: включають унікальний ID об'єкта, геопросторові параметри (широта, довгота), адміністративне розташування (адреса, код регіону), функціональну категорію (тип об'єкта);

– тимчасові пари візуальних перспектив (багатовидовий масив): структуровані для поєднання історичних передоб'єктних виглядів (Before_Front, Before_Back, Before_Left, Before_Right) з перспективними виглядів після пошкодження (After_Front, After_Back, After_Left, After_Right, After_Iso). Ізометрична проєкція (After_Iso) включена явно для підтримки подальшої оцінки глибини фізичних куп уламків;

– адміністративні записи та записи «ground truth»: документують індикатори статусу даних, умови ліцензування, збирачів даних та верифікований цільовий клас, присвоєний експертом (Damage).

Дотримуючись цієї схеми, ми скомпілювали загалом 108 унікальних тестових активів. Розподіл цільових міток серед цих тестових зразків проілюстровано на рис. 3.

Розподіл зміщений у бік рівнів пошкоджень від помірних до важких (клас 3 становить 42 одиниці, або 38,9 % набору даних), що відображає реальні фізичні умови, де удари спричиняють значні структурні компроміси без повного руйнування. Класи незначних пошкоджень та повного обвалення (Клас 0 та Клас 4) зустрічаються рідше (13,9 % та 11,1 % відповідно). Для оцінки ефективності запропонованої методології оцінки пошкоджень з багатьох ракурсів були проведені експерименти з використанням однієї звичайної моделі глибокого навчання та чотирьох сучасних мультимодальних великих ВММ.

Вибрані моделі представляють різні архітектурні парадигми, що дозволяє провести порівняльний аналіз між підходом керованого комп'ютерного зору та нещодавніми мультимодальними ШІ-системами загального призначення. Короткий огляд оцінюваних моделей представлено в табл. 1.

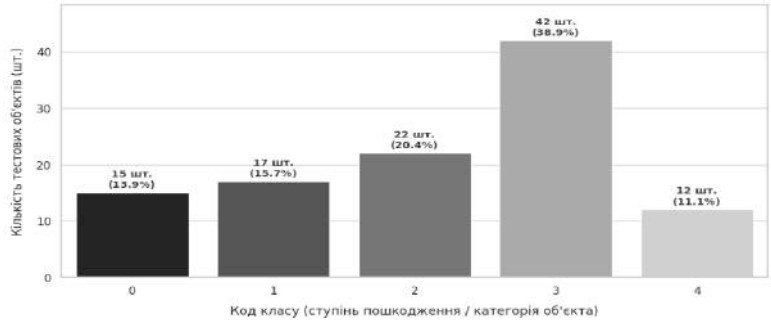


Рисунок 3. Початковий розподіл класів ground truth у тестовому наборі

Таблиця 1

Оцінювані моделі ШІ, що використовуються для класифікації пошкоджень інфраструктури

Модель	Категорія	Короткий опис
Unet + ResNet	Deep Learning	Спеціалізована модель комп'ютерного зору з симетричною архітектурою «кодер-декодер»
GPT-5.5 (High Intelligence)	Vision-Language Model	Мультимодальна велика мовна модель OpenAI
Claude Sonnet 5 (Medium)	Vision-Language Model	Мультимодальна модель Anthropic
Gemini 3.1 Pro (High)	Vision-Language Model	Мультимодальна базова модель Google
Grok 4 (Fast)	Vision-Language Model	Мультимодальна модель xAI

Продуктивність кожної оцінюваної моделі аналізувалася за допомогою шести додаткових метрик. Разом ці метрики забезпечують комплексне оцінювання як загальної ефективності класифікації, так і типів помилок прогнозування, зроблених моделями:

– Accuracy (точність) – вимірює загальну частку правильно класифікованих інфраструктурних об’єктів;

– Weighted Precision (зважена прецизійність) – оцінює надійність прогнозованих класів пошкоджень з урахуванням розподілу класів;

– Weighted Recall (зважена повнота) – вимірює здатність моделі правильно ідентифікувати об’єкти, що належать до кожної категорії пошкоджень;

– Macro F1-score (макро F1-показник) – забезпечує збалансовану оцінку, розглядаючи всі класи пошкоджень як рівноцінні, що робить її особливо придатною для незбалансованих наборів даних;

– Overestimation ratio (коефіцієнт переоцінки) – представляє частку прогнозів, де присвоєний клас пошкодження вищий за мітку ground-truth;

– Underestimation ratio (Коефіцієнт недооцінки) – представляє частку прогнозів, де присвоєний клас пошкодження нижчий за мітку ground-truth.

Для виконання систематичного кількісного оцінювання прогнозовані виводи, згенеровані на всьому тестовому наборі, були скомпільовані в

централізовану базу даних. Порівняльні метрики були обчислені для оцінки точності класифікації, прецизійності, повноти та збалансованих значень F1-macro для кожної моделі. Крім того, ми відстежували тенденції інженерних помилок, зокрема рівень переоцінки (гіперболізації) та недооцінки (пом'якшення) для оцінки безпеки та надійності кожного підходу. Порівняльні результати продуктивності оцінюваних моделей узагальнено в табл. 2. З метою емпіричної перевірки статистичної надійності зафіксованих показників загальної точності було побудовано 95 %-ві довірчі інтервали за критерієм Вілсона: для флагманських систем Claude та Gemini розрахунковий діапазон склав [0,545; 0,723], для конфігурації Grok – [0,452; 0,637], для моделі ChatGPT – [0,443; 0,628], а для референтного сегментаційного конвеєра U-Net – [0,319; 0,501]. Зіставлення меж отриманих інтервалів свідчить про наявність статистично достовірної переваги провідних VLM (Claude та Gemini) над базовим пайплайном U-Net, оскільки мінімальна границя довірчого інтервалу лідерів (0,545) строго вища за максимальне значення для моделі сегментації (0,501).

Таблиця 2

Зведена оцінка ефективності моделей

Модель	Acc	Prec (W)	Rec (W)	F1-Macro	Over-est. Ratio	Under-est. Ratio
Claude	0,639	0,674	0,639	0,639	0,176	0,185
Gemini	0,639	0,691	0,639	0,570	0,231	0,130
Grok	0,546	0,563	0,546	0,527	0,343	0,111
ChatGPT	0,537	0,550	0,537	0,515	0,315	0,148
Unet	0,407	0,424	0,407	0,348	0,398	0,194

Натомість у сегменті рішень проміжного рівня (Grok і ChatGPT) спостерігається виражений перетин інтервальних меж із показниками U-Net. Таке нашарування довірчих смуг дає підстави констатувати відсутність статистично відокремленого розриву між середніми мультимодальними мережами та локалізованим CV-алгоритмом за наявного обсягу експериментальної вибірки. Розглянемо детальніше класифікаційні звіти та матриці невідповідностей класифікації кожної з моделей. Модель Claude (рис. 4, табл. 3) продемонструвала бездоганну точність ідентифікації цілих споруд (Precision = 1,000 для Класу 0) та збалансовану чутливість щодо зон критичних руйнувань. Її головною перевагою є здатність розділяти межу між важкими пошкодженнями та повним колапсом: для Класу 3 та Класу 4 показники Precision досягли 0,740 та 0,750 відповідно. Основні похибки зосереджені в зоні помірних пошкоджень (Клас 1 і Клас 2), де понад 58 % об'єктів із незначними дефектами було класифіковано як помірні пошкодження через чутливість моделі до локальних розбиттів вікон і слідів уламків.

ChatGPT характеризується суттєвою асиметрією (рис. 5, табл. 4): система ефективно розпізнає неушкоджені будівлі (Recall = 0,930), проте відчуває системні труднощі у градації деструкцій.

Зокрема, повнота для Класу 1 знизилася до 0,240 через масове помилкове зміщення у бік Класу 2 (58,8 % випадків). Найбільш проблемним сегментом виявився Клас 4, де точність становить лише 0,250: у двох третинах випадків

(66,7 %) повністю знищені об'єкти трактувалися моделлю як пошкодження 3-го ступеня, що свідчить про розмивання меж інженерної оцінки руїн.

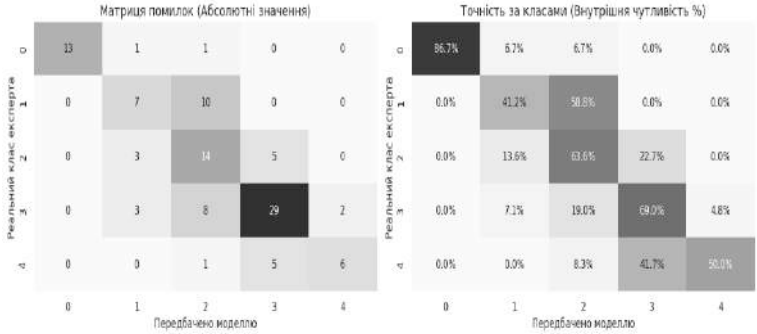


Рисунок 4. Матриця невідповідностей моделі Claude

Таблиця 3

Класифікаційний звіт моделі Claude

Клас / Метрика	Precision	Recall	F1-Score	Support
Клас 0	1,000	0,870	0,930	15
Клас 1	0,500	0,410	0,450	17
Клас 2	0,410	0,640	0,500	22
Клас 3	0,740	0,690	0,720	42
Клас 4	0,750	0,500	0,600	12
Accuracy	–	–	0,640	108
Macro Average	0,680	0,620	0,640	108
Weighted Average	0,670	0,640	0,650	108

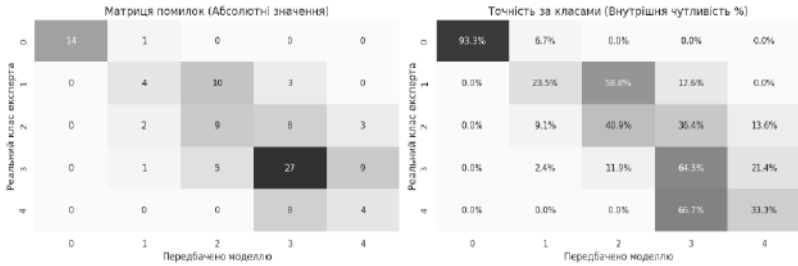


Рисунок 5. Матриця невідповідностей моделі ChatGPT

Модель Gemini (рис. 6, табл. 5) виявила яскраво виражений консервативний профіль класифікації, спрямований на попередження пропуску аварійного стану. Повнота виявлення Класу 3 сягнула рекордних 0,900 (38 із 42 об'єктів), що з інженерної точки зору зводить до мінімуму небезпеку недооцінювання руйнувань несних конструкцій, проте це досягається за рахунок стягування сусідніх категорій: модель перенаправляє до Класу 3 рівно половину об'єктів Класу 2 (50,0 %) та переважну більшість зруйнованих будівель Класу 4 (83,3 %).

Таблиця 4

Класифікаційний звіт моделі ChatGPT

Клас / Метрика	Precision	Recall	F1-Score	Support
Клас 0	1,000	0,930	0,970	15
Клас 1	0,500	0,240	0,320	17
Клас 2	0,380	0,410	0,390	22
Клас 3	0,590	0,640	0,610	42
Клас 4	0,250	0,330	0,290	12
Accuracy	–	–	0,540	108
Macro Average	0,540	0,510	0,520	108
Weighted Average	0,550	0,540	0,530	108

Як наслідок, Recall для Класу 4 впав до 0,170, хоча всі сформовані щодо нього прогнози були абсолютно точними (Precision = 1,000).

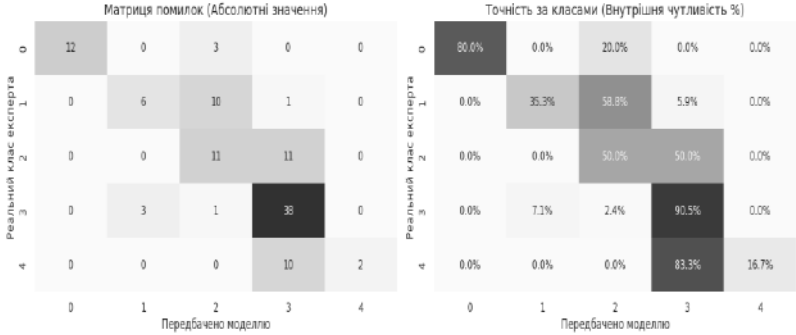


Рисунок 6. Матриця невідповідностей моделі Gemini

Аналіз матриці моделі Grok (рис. 7, табл. 6) фіксує системну схильність до гіпердіагностики пошкоджень. Окрім помірного розпізнавання Класів 1 і 2, модель помилково віднесла 54,5 % будівель Класу 2 до значно небезпечнішого Класу 3.

Таблиця 5

Класифікаційний звіт моделі Gemini

Клас / Метрика	Precision	Recall	F1-Score	Support
Клас 0	1,000	0,800	0,890	15
Клас 1	0,670	0,350	0,460	17
Клас 2	0,440	0,500	0,470	22
Клас 3	0,630	0,900	0,750	42
Клас 4	1,000	0,170	0,290	12
Accuracy	–	–	0,640	108
Macro Average	0,750	0,540	0,570	108
Weighted Average	0,690	0,640	0,610	108

Одночасно повністю зруйновані будівлі (Клас 4) у 66,7 % випадків були ідентифіковані як пошкодження попереднього рівня. Це зумовило низьку точність (Precision = 0,270) та помірний показник F1-score (0,300) для категорії тотального знищення споруд.

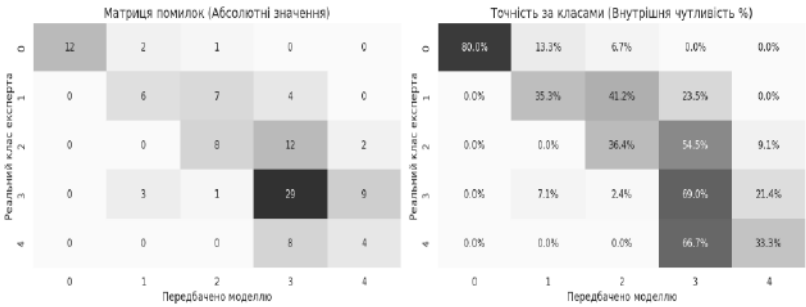


Рисунок 7. Матриця невідповідностей моделі Grok

Таблиця 6

Класифікаційний звіт моделі Grok

Клас / Метрика	Precision	Recall	F1-Score	Support
Клас 0	1,000	0,800	0,890	15
Клас 1	0,550	0,350	0,430	17
Клас 2	0,470	0,360	0,410	22
Клас 3	0,550	0,690	0,610	42
Клас 4	0,270	0,330	0,300	12
Accuracy	–	–	0,550	108
Macro Average	0,570	0,510	0,530	108
Weighted Average	0,560	0,550	0,540	108

Поведінка референтної моделі комп'ютерного зору U-Net (рис. 8, табл. 7) виявляє специфічну проблему, що випливає з умов формування навчальної вибірки. Повнота розпізнавання неушкодженого Класу 0 склала лише 0,200: із 15 абсолютно цілих будівель модель правильно класифікувала лише 3 об'єкти, хибно ідентифікувавши решту як пошкоджені споруди Класів 1, 2 і 3. Оскільки сегментатор навчався виключно на фрагментах уражених фасадів без доступу до геометричних еталонів норми, природні тіні, відлущення фарби чи неоднорідні текстури стін були інтерпретовані мережею як деструкції. Водночас у зоні реальних середніх та важких деструкцій (Класи 2–4) алгоритм працює стабільно: повнота виявлення Класу 3 становить 0,600, а Класу 4 – 0,420, що за чутливістю перевершує ChatGPT і Gemini.

Експериментальні результати демонструють чіткий розрив у продуктивності між моделями високого рівня міркування та базовою установкою сегментації:

– продуктивність вищого рівня: Claude та Gemini досягли найвищої загальної точності 0,639. Claude продемонстрував найбільш збалансовану поведінку класифікації з F1-Macro 0,639 та низьким коефіцієнтом переоцінки 0,176. Навпаки, Gemini досяг найвищої зваженої прецизійності 0,691, зберігаючи критичні помилки недооцінки (пом'якшення) на рівні 0,130;

– моделі середнього рівня: Grok та ChatGPT показали помірну продуктивність із точністю 0,546 та 0,537 відповідно, та значеннями F1-Macro

трохи вище 0,515. Проте обидві моделі страждали від підвищених коефіцієнтів переоцінки, що перевищували 0,310, що призводило до частих хибних тривог;

– обмеження базової лінії та пом'якшення: Базова установка Unet значно відставала, зареєструвавши низьку точність 0,407 та збалансований F1-Macro 0,348. Ця база була схильна до переоцінки рівнів пошкоджень з коефіцієнтом 0,398.

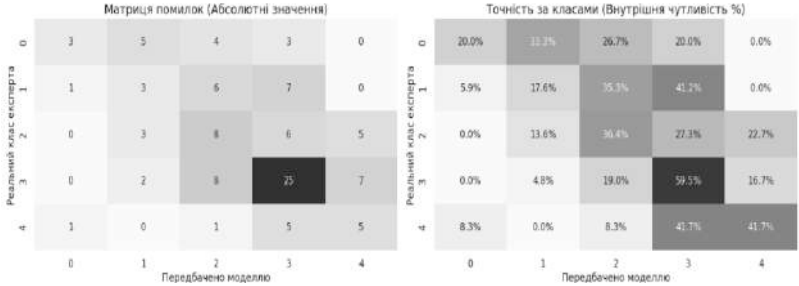


Рисунок 8. Матриця невідповідностей моделі Unet Resnet

Таблиця 7

Класифікаційний звіт моделі Unet Resnet

Клас / Метрика	Precision	Recall	F1-Score	Support
Клас 0	0,600	0,200	0,300	15
Клас 1	0,230	0,180	0,200	17
Клас 2	0,300	0,360	0,330	22
Клас 3	0,540	0,600	0,570	42
Клас 4	0,290	0,420	0,340	12
Accuracy	–	–	0,410	108
Macro Average	0,390	0,350	0,350	108
Weighted Average	0,420	0,410	0,400	108

7. Висновки та перспективи

Це дослідження представило порівняльне оцінювання ВММ високого рівня та кастомізованої базової лінії семантичної сегментації для класифікації пошкоджень інфраструктури за наземними знімками. Експериментальні результати підтверджують, що передові моделі міркування досягають сильної прогнозної продуктивності у складних завданнях структурного парсингу.

Claude продемонстрував найбільш надійну та математично збалансовану поведінку класифікації, забезпечивши найвищу точність (0,639) та збалансований F1-Macro (0,639). Критично важливо, що Claude виявився здатним чітко розмежовувати сильно розмиту межу між Класом 3 (Значні пошкодження) та Класом 4 (Зруйнований), досягнувши високої прецизійності 0,740 та повноти 0,690 на домінуючій підмножині Класу 3 (Support = 42). Gemini зрівнявся з піковою точністю Claude 0,639 і продемонстрував вищу зважену прецизійність 0,691. Gemini виявився найбільш консервативною, орієнтованою на інженерні потреби моделлю, зафіксувавши найнижчий коефіцієнт недооцінки (0,130). Ця поведінка підтверджується винятково високою повнотою 0,900 для Класу 3, що мінімізує катастрофічні структурні хибнонегативні результати, хоча він виявив тенденцію згортати випадки Класу

4 у прогнози Класу 3 (повнота лише 0,170 для Класу 4). Grok та ChatGPT посіли помірний рівень з точністю 0,546 та 0,537 відповідно. Обидві моделі страждали від підвищених коефіцієнтів переоцінки, що перевищували 0,310, часто класифікуючи незначні естетичні поверхневі аномалії як значні структурні обвали. Базова U-Net (ResNet Backbone) продемонструвала глобально низькі результати з точністю 0,407 та F1-macro 0,348. Ця база зареєструвала високий коефіцієнт переоцінки 0,398. Матриця невідповідності показує, що ця помилка фундаментально пов'язана з нездатністю ідентифікувати неушкоджені структури (прецизійність Класу 0 – 0,600, повнота – 0,200), спричинена безпосередньо обмеженням набору даних, де навчальні маски містили лише «пост-пошкоджені» зображення. Однак коефіцієнт недооцінки локалізованого піксельного сегментатора (0,194) залишався порівнянним з найкращими ВММ. Рекомендується розглянути використання базової моделі без класу неушкоджених структур для оцінки незалежної можливості визначення пошкоджень.

Розроблений фреймворк багатовидової класифікації служить основним механізмом прийняття рішень для інтелектуальної багатофункціональної ГІС. Локалізовані прогнози структурних класів та розподіли необроблених пікселів, згенеровані цією моделлю, безпосередньо сприймаються наступними компонентами системи:

– автоматизована оцінка матеріалів: система зіставляє присвоєний клас пошкодження (0–4) з локалізованими архетипами будівель, перетворюючи площі пікселів на оцінки об'ємів бетону для фракцій будівельних відходів (наприклад, подрібнений бетон, пил цегляної кладки та брухт структурного скління);

– оптимізація логістики: ці оцінки об'єму фізичних відходів перехресно посилаються на просторові координати (широта, довгота) всередині географічної бази даних. Інтелектуальний механізм підтримки рішень багатофункціональної ГІС потім динамічно спрямовує автопарки знесення, зіставляючи оцінені запаси відходів з найближчими центрами перероблення та рециклінгу для зниження регіональних транспортних витрат.

Подальша робота буде зосереджена на розширенні бази даних ground-truth для включення рівного балансу неушкоджених геометрій будівель до катастроф. Перенавчання U-Net на основі патчів з використанням цих еталонних зразків усуне поточне зміщення переоцінки щодо ознак Класу 0. Враховуючи малий обсяг та низьку затримку, цей локалізований сегмент представляє варіант високомасштабованого крайового розгортання для польових операцій у реальному часі.

Подяки

Це дослідження було профінансовано Міністерством освіти і науки України в рамках науково-дослідної роботи «Розробка інтелектуальної багатофункціональної геоінформаційної системи для інвентаризації будівельних відходів при відбудові пошкоджених війною інфраструктурних об'єктів» (номер державної реєстрації 0126U001737). Автори також висловлюють подяку А. Барановій, Б. Іпатову та Д. Паласу за їхню цінну

допомогу у зборі набору зображень пошкоджень війною та проведенні експериментів з порівняльного аналізу ВММ.

Література

[1] Samal, C. G., Biswal, D. R., Udgata, G., & Pradhan, S. K. (2025). Estimation, Classification, and Prediction of Construction and Demolition Waste Using Machine Learning for Sustainable Waste Management: A Critical Review. *Construction Materials*, *5*(1), 10. https://doi.org/10.3390/constrmater5010010.

[2] Gupta, R., Hosfelt, R., Sajeev, S., Patel, N., Goodman, B., Doshi, J., Heim, E., Choset, H., & Gaston, M. (2019). Xbd: A dataset for assessing building damage from satellite imagery. *arXiv*. https://doi.org/10.48550/ARXIV.1911.09296.

[3] Klym, Y. (2025). Assessment of damage to Ukrainian infrastructure using satellite imagery [Bachelor's thesis, Ukrainian Catholic University]. https://hdl.handle.net/20.500.14570/5516.

[4] Molchanova, M., Didur, V., Mazurets, O., Sobko, O., & Zakharkevich, O. (2025). Method for construction and demolition waste classification using two-factor neural network image analysis. In N. Shakhovska, A. T. Augousti, S. Liaskovska, & O. Duran (Eds.), *Proceedings of the 2nd International Conference on Smart Automation & Robotics for Future Industry (SMARTINDUSTRY 2025)* (Vol. 3970, pp. 168–182). CEUR. https://ceur-ws.org/Vol-3970/PAPER14.pdf.

[5] Guo, S., Cockayne, M. J., Ortolani, M., Al-Hamd, R., & Al-Bander, B. (2025). Zero-shot crack segmentation for structural health monitoring using class activation map guided segment anything model. https://doi.org/10.2139/ssrn.5197086.

[6] Zheng, Z., Zhong, Y., Wang, J., Ma, A., & Zhang, L. (2021). Building damage assessment for rapid disaster response with a deep object-based semantic change detection framework: From natural disasters to man-made disasters. *Remote Sensing of Environment*, *265*, 112636. https://doi.org/10.1016/j.rse.2021.112636.

[7] Duarte, D., Nex, F., Kerle, N., & Vosselman, G. (2018). Multi-resolution feature fusion for image classification of building damages with convolutional neural networks. *Remote Sensing*, *10*(10), 1636. https://doi.org/10.3390/rs10101636.

[8] Estêvão, J. M. C. (2024). Effectiveness of generative ai for post-earthquake damage assessment. *Buildings*, *14*(10), 3255. https://doi.org/10.3390/buildings14103255.

[9] K. Alimi, R. Jin, B. N. Nguyen, Q. Nguyen, W. Chen, & L. Hosking. (2025). Exploring artificial intelligence applications in construction and demolition waste management: A review of existing literature. *Journal of Science and Transport Technology*, 104–136. https://doi.org/10.58845/jstt.utt.2025.en.5.1.104-136.

[10] Dadiverina, L., Laukhin, D., Hryhoriev, O., Khalymendyk, D., & Bondarenko, V. (2024). Management of construction waste generated by military actions: Analysis and solutions. *Collection of Research Papers of the National Mining University*, *79*, 163—174. https://doi.org/10.33271/crpnmu/79.163.

[11] Aouf, R. S. (2025, July 7). *Circularity on the Edge AI finds reusable materials in rubble of Ukrainian buildings*. Dezeen. https://www.dezeen.com/2025/07/07/circularity-on-the-edge-ai-ukraine/.

[12] Aimaiti, Y., Sanon, C., Koch, M., Baise, L. G., & Moaveni, B. (2022). War related building damage assessment in kyiv, ukraine, using sentinel-1 radar and sentinel-2 optical images. *Remote Sensing*, *14*(24), 6239. https://doi.org/10.3390/rs14246239.

[13] Lysanets, A., Kosukha, O., Panchenko, T., & Tereshchenko, Y. (2026). Embedding-enhanced u-net with a patch-based approach and a novel dataset for ground-level building damage segmentation. *Applied Artificial Intelligence*, *40*(1), 2685357. https://doi.org/10.1080/08839514.2026.2685357.

[14] Arsirii, O., Ivanov, O., Bieliaiev, K., & Cudecka-Purina, N. (2025). Intelligent information technology for inventory and utilization of construction and demolition waste from damaged infrastructure facilities, in: L. David, Y. Kondratenko, V. Vychuzhanin, H. Yin & N. Rudnichenko (Eds.), *Proceedings of the 13-th International Conference on Information Control Systems & Technologies (ICST 2025)* (Vol. 4048, pp. 276–289). CEUR. https://doi.org/10.55056/ceur-ws.org/Vol-4048/paper22.pdf.

[15] Lysanets, A. (2025). Ukrainian Building Damage Assessment System: Ground-level Ukrainian Building Damage Segmentation Dataset [Dataset]. https://www.kaggle.com/datasets/andrewlysanets/ukrainian-damaged-buildings/data.

COMPARATIVE ANALYSIS OF VLM FOR INFRASTRUCTURE DAMAGE CLASSIFICATION: A CASE STUDY OF UKRAINE

Ph.D., Ivanov O.[1], Bieliaiev K. [2], Oliinyk V. [3], Arsiriy O.[4]
[1,2,3]Odesa Polytechnic National University, Ukraine,
[4]Odesa State Maritime University, Ukraine

Abstract*. The large-scale destruction of civil infrastructure caused by the war in Ukraine has created an urgent need for automated, reliable, and scalable methods for structural damage assessment. This study presents a comparative evaluation of Vision-Language Models (VLM) and a hybrid computer vision approach for multi-view infrastructure damage classification. A specialized dataset was constructed using ground-level images of war-damaged buildings collected from multiple regions of Ukraine, where each infrastructure object is represented by 2 to 8 photographs, including pre- and post-damage views when available. Damage severity is categorized into 5 classes ranging from undamaged to completely destroyed. The proposed methodology integrates a multi-view reasoning framework with semantic segmentation based on a U-Net architecture employing a ResNet encoder and a rule-based heuristic model that estimates structural damage using pixel-level metrics. Multi-view evidence is aggregated to produce a single object-level assessment, reducing ambiguity caused by occlusions and limited viewing angles. The proposed approach was experimentally compared with several advanced multimodal VLMs (GPT-5.5, Claude Sonnet 5, Gemini 3.1 Pro, Grok 4), using Accuracy, Precision, Recall, F1-score, and overestimation-underestimation ratios. Experimental evaluation conducted on a dedicated dataset of 108 infrastructure objects demonstrates that advanced VLMs outperform the baseline segmentation model in overall classification accuracy while providing robust reasoning across complex structural damage scenarios. At the same time, the proposed hybrid segmentation-based framework offers interpretable pixel-level damage estimation and remains suitable for resource-constrained deployments. The developed multi-view assessment methodology constitutes a core analytical component of an intelligent multifunctional GIS designed to support construction and demolition waste inventory, optimize recycling logistics, and facilitate sustainable post-war reconstruction based on circular economy principles.*

Keywords*. Infrastructure damage assessment, Vision-Language Models, multi-view image analysis, semantic segmentation, construction and demolition waste, artificial intelligence, machine learning.*

UDC 004.8:004.75:004.021
DOI

МЕТОД ІНТЕЛЕКТУАЛЬНОГО РИЗИК-ОРІЄНТОВАНОГО АНАЛІЗУ МУЛЬТИМОДАЛЬНИХ БАГАТОВИМІРНИХ ДАНИХ ДЛЯ АДАПТИВНОГО КЕРУВАННЯ РЕСУРСАМИ ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖ

Ph.D., Рудніченко М.[1][0000-0002-7343-8076], Ph.D., Шибаєва Н. [2][0000-0002-7869-9953], Шумейко К.[2][0009-0002-1523-9789], Шведов Д.[4][0009-0002-4823-8782], Зленський А.[5][0009-0008-9784-2963], Dr.Sci., Петров І.[6][0000-0002-8740-6198]

[1-6]Національний університет «Одеська Політехніка»,
[7]Національний університет «Одеська морська академія»
EMAIL: [1]nickolay.rud@gmail.com, [2]nati.sh@gmail.com, [3]kshumeyko@gmail.com, [4]frumle@ukr.net,[5]studylearnerstudy@gmail.com, [6]firmn@gmail.com

Аннотація. *У статті представлено дослідження щодо розроблення методу інтелектуального ризик-орієнтованого аналізу мультимодальних багатовимірних даних для адаптивного керування ресурсами децентралізованих мереж із використанням глибинного навчання та механізмів адаптивного злиття інформації. Актуальність дослідження обґрунтована зростанням обсягів неоднорідних даних у розподілених цифрових середовищах та необхідністю одночасного забезпечення достовірності ризикового аналізу, оперативності обробки інформації та раціонального використання обмежених обчислювальних, комунікаційних і енергетичних ресурсів. У роботі проаналізовано обмеження традиційних стратегій мультимодального злиття та обґрунтовано доцільність використання адаптивної архітектури, яка враховує поточну якість інформаційних модальностей і рівень ризику під час формування керувальних рішень. Запропонований метод поєднує модально-специфічне кодування даних, адаптивне зважування інформаційних потоків, формування інтегрованого латентного представлення, оцінювання ризикового стану та замкнений контур керування ресурсами децентралізованої мережі. Експериментальний стенд реалізовано із використанням Python, Jupyter Notebook, NumPy, Pandas, Scikit-learn, PyTorch та Matplotlib. Для формування експериментального інформаційного середовища використано відкриті реальні набори даних IEEE-CIS Fraud Detection, Online Retail та Default of Credit Card Clients, що містять транзакційні, часові, поведінкові, клієнтські та ідентифікаційні характеристики. Проведено порівняння запропонованого методу з підходами раннього, пізнього та статичного зваженого злиття за показниками F1-міри, ROC-AUC, затримки обробки та енергетичних витрат. Додатково виконано дослідження стійкості методів до зростання ресурсного навантаження та абляційний аналіз основних компонентів архітектури. Отримані результати демонструють переваги запропонованого підходу щодо поєднання якості ризикового аналізу, адаптивності та ефективності використання ресурсів, що підтверджує перспективність його застосування у децентралізованих інтелектуальних мережах.*

Ключові слова: *мультимодальне об'єднання даних, інтелектуальний аналіз даних, ризик-орієнтований аналіз, адаптивне управління ресурсами, децентралізовані мережі, глибоке навчання, гібридне моделювання, латентне представлення*

Вступ

Інтенсивний розвиток цифрових технологій, розподілених обчислювальних середовищ та інтелектуальних систем прийняття рішень зумовлює постійне

ускладнення інформаційного простору, в якому функціонують сучасні автоматизовані системи. Зростання кількості джерел інформації, збільшення швидкості формування даних та поява нових способів їх отримання створюють умови, за яких традиційні методи оброблення окремих інформаційних потоків не забезпечують необхідного рівня оперативності та обґрунтованості керуючих рішень. Особливої актуальності ця проблема набуває для децентралізованих мереж, у яких значна частина даних формується безпосередньо на периферійних вузлах, а прийняття рішень має відбуватися в умовах обмежених обчислювальних, енергетичних і комунікаційних ресурсів.

Специфіка сучасних інформаційно-керуючих систем полягає у тому, що дані, які характеризують їхній стан, мають неоднорідну природу. Вони можуть бути представлені числовими параметрами, часовими рядами, сигналами сенсорів, просторовими характеристиками, структурованими записами, повідомленнями мережевих вузлів та іншими інформаційними представленнями. Кожен із таких типів даних відображає лише окремий аспект досліджуваного процесу, його інформативність залежить від поточного стану системи та умов функціонування джерела інформації. У результаті виникає необхідність накопичувати різнорідні дані, забезпечувати їх узгоджене представлення, визначати ступінь їхньої інформативності та враховувати взаємозв'язки між окремими інформаційними потоками.

Відповідний напрям досліджень сформувався у межах концепції мультимодального аналізу даних (МАД), яка передбачає спільне використання інформації різної природи для формування більш повного представлення досліджуваного об'єкта або процесу. На відміну від традиційного підходу, за якого кожне джерело аналізується незалежно, МАД дає змогу використовувати взаємодоповнювальні властивості інформаційних потоків. При цьому ефективність інтеграції визначається кількістю доступних модальностей, здатністю моделі враховувати відмінності у структурі, часовій організації, достовірності та інформаційній цінності даних. Дослідження у сфері глибинного МАД підтверджують, що поєднання різних представлень може істотно розширювати можливості інтелектуальної системи, однак одночасно створює додаткові проблеми, пов'язані з узгодженням ознак, синхронізацією інформації, неповнотою даних та наявністю шумів [1, 2, 3, 4].

У цьому контексті особливого значення набуває поняття ризику. Для інформаційно-керуючої системи ризик доцільно розглядати ширше, ніж традиційну ймовірність виникнення фінансових втрат. Він може характеризувати ймовірність переходу системи до небажаного стану, погіршення якості функціонування, перевищення допустимого навантаження, виникнення затримок, втрати доступності інформаційного ресурсу або неефективного використання наявних можливостей. Такий підхід дозволяє перенести методологію інтелектуального аналізу ризиків на більш широкий клас розподілених систем, у яких необхідно прогнозувати майбутні значення певних параметрів та потенційні наслідки поточного стану системи.

Фінансові інформаційні системи є показовим прикладом середовища, в якому прийняття рішень безпосередньо залежить від своєчасної оцінки ризику. Фінансові дані характеризуються високою динамічністю, нелінійністю,

неоднорідністю та залежністю між окремими параметрами. Крім того, для оцінювання ризикових станів часто необхідно одночасно враховувати історичні часові залежності, структуровані характеристики об'єктів, поведінкові ознаки та зовнішні фактори. Саме тому у фінансовій аналітиці активно розвиваються методи машинного (МН) та глибинного навчання (ГН), здатні виявляти складні нелінійні закономірності та формувати прогностичні оцінки на основі великих масивів даних [5, 6, 7, 8]. Водночас перенесення таких підходів до розподілених інформаційних середовищ потребує їх адаптації до умов мультимодальності, децентралізації та ресурсних обмежень.

Принциповою особливістю у контексты дослідження є трактування ризикової оцінки не як кінцевого результату інтелектуального аналізу, а як інформаційного сигналу для подальшого формування керуючого рішення. Якщо традиційна система аналізу завершує роботу після визначення класу або числового показника ризику, то в розподіленому середовищі отримана оцінка може бути використана для зміни режиму функціонування окремих вузлів, перерозподілу обчислювального навантаження, зміни пріоритетів передавання інформації або адаптації параметрів оброблення даних. Необхідність такого підходу особливо виражена у децентралізованих IoT-мережах та edge-середовищах. На відміну від централізованої архітектури, у якій значна частина інформації може передаватися до потужного серверного центру, децентралізована мережа передбачає розподіл обчислювальних функцій між великою кількістю вузлів. Кожен вузол може мати власні обмеження щодо продуктивності процесора, обсягу пам'яті, енергоспоживання та пропускної здатності каналу зв'язку. Додатково виникає проблема нерівномірного навантаження, оскільки інтенсивність надходження інформації та складність її оброблення можуть істотно змінюватися в часі. За таких умов статичний розподіл ресурсів не здатний адекватно реагувати на зміну інформаційного та ризикового стану системи [9, 10, 11, 12].

Застосування методів інтелектуального керування ресурсами дозволяє перейти від фіксованої конфігурації до адаптивного режиму функціонування. Перспективним інструментом у цьому напрямі є навчання з підкріпленням, яке дає можливість формувати політику прийняття рішень на основі взаємодії агента з динамічним середовищем. Зокрема, ГН з підкріпленням використовується для задач розподілу обчислювальних ресурсів, вибору способу розвантаження обчислень, керування передаванням даних та оптимізації роботи edge-вузлів [9,10]. Проте застосування таких методів лише до ресурсних параметрів не враховує повною мірою інформаційну невизначеність, яка виникає під час формування стану середовища. Якщо керуюча модель отримує неповне, суперечливе або недостатньо достовірне представлення стану, навіть оптимальна з погляду ресурсів дія може призвести до небажаного результату.

Саме тому доцільно поєднати МАД, оцінювання ризику та адаптивне керування ресурсами в межах єдиного інтелектуального підходу до аналізу даних. Така інтеграція передбачає, що на першому етапі система отримує інформацію з декількох джерел, після чого виконується її попереднє узгодження та оцінювання якості. На наступному етапі для кожної модальності

формується відповідне латентне представлення, яке відображає найбільш інформативні характеристики вихідного потоку. Отримані представлення інтегруються з урахуванням їхньої поточної значущості, унаслідок чого формується узагальнений вектор стану системи. На його основі визначається рівень ризику, який у подальшому використовується разом із поточними характеристиками доступних ресурсів для формування адаптивного рішення. Така структура визначає специфіку поняття гібридності, яке використовується в роботі. Гібридність не обмежується механічним поєднанням декількох алгоритмів МН, розглядається як поєднання різних механізмів представлення, інтеграції, оцінювання та прийняття рішень. Для різних типів даних можуть використовуватися різні способи вилучення ознак, оскільки характер інформації визначає доцільність відповідного математичного апарату. Часові послідовності потребують урахування залежностей між попередніми та поточними станами, структуровані дані можуть ефективно оброблятися моделями табличного представлення, а інформація, що характеризує взаємодію між вузлами, природно подається у вигляді графових структур. Після цього результати окремих моделей можуть бути інтегровані таким чином, щоб поточна якість та інформативність кожної модальності безпосередньо впливали на її внесок у загальне рішення.

Важливою проблемою при цьому є забезпечення стійкості інтелектуальної системи до неповноти інформації. У реальних розподілених середовищах окремий інформаційний канал може тимчасово втрачатися, містити пропуски або характеризуватися підвищеним рівнем шуму. Якщо всі модальності мають фіксовані ваги, деградація одного джерела безпосередньо впливає на кінцеву оцінку. Адаптивний механізм інтеграції дає змогу змінювати внесок окремих джерел залежно від поточного стану даних. За такого підходу мультимодальна система використовує додаткову інформацію, отримує можливість частково компенсувати ненадійність окремих інформаційних каналів за рахунок інших джерел. Ще одним важливим аспектом є врахування невизначеності при формуванні ризикової оцінки. У практичних задачах одна й та сама сукупність ознак може відповідати декільком можливим сценаріям розвитку системи, а межі між нормальним та ризиковим станом не завжди мають чіткий характер. Тому використання лише детермінованої класифікації може бути недостатнім для прийняття керуючих рішень. Більш доцільним є формування ризикового показника, який відображає ступінь наближення системи до небажаного стану та може використовуватися разом із оцінкою достовірності отриманої інформації. Такий підхід відповідає сучасній тенденції розвитку «trustworthy та explainable artificial intelligence,» де поряд із прогнозною якістю розглядаються надійність, інтерпретованість і відповідальність алгоритмічних рішень [6]. Поєднання МАД з ризик-орієнтованим керуванням дає можливість змінити саму логіку розподілу ресурсів. У традиційному підході ресурсний стан визначається переважно на основі поточного навантаження, кількості завдань та доступної продуктивності вузлів. У контексті дослідження до цього набору може бути додано інформацію про ризиковий стан. Якщо інтелектуальний аналіз виявляє підвищення ризику для певного процесу, вузла або інформаційного потоку, система може збільшити пріоритет його оброблення,

виділити додатковий обчислювальний ресурс або змінити маршрут передавання відповідних даних. За низького рівня ризику, навпаки, частина ресурсів може бути перенаправлена до інших завдань. У результаті ресурсна політика стає залежною не лише від кількісних характеристик навантаження, а й від потенційних наслідків невчасного або недостатньо якісного оброблення інформації. Окремої уваги потребує проблема розподіленого навчання моделей. Передавання всіх первинних даних до централізованого вузла не завжди є доцільним через обмеження пропускної здатності мережі, обчислювальні витрати та вимоги до збереження локальності інформації. Одним із можливих шляхів вирішення цієї проблеми є використання федеративного навчання, за якого локальні вузли виконують навчання або донавчання моделей на власних даних, а централізовано або децентралізовано узгоджуються параметри моделі [11, 15].

Розв'язання зазначених проблем потребує переходу від ізольованого використання моделей інтелектуального аналізу до інтегрованого підходу, здатного одночасно враховувати різнорідність інформації, її поточну достовірність, рівень ризику та ресурсні обмеження середовища. У цьому випадку результатом роботи інтелектуальної системи має бути не тільки прогноз або класифікація, а обґрунтована адаптивна дія, вибір якої визначається поточним станом інформаційного та ресурсного середовища.

З огляду на зазначене, у роботі пропонується метод інтелектуального ризик-орієнтованого аналізу МАД для адаптивного керування ресурсами децентралізованих мереж. Метод базується на послідовному поєднанні процедур підготовлення різнорідної інформації, формування модальних представлень, адаптивної інтеграції ознак, оцінювання ризикового стану та вибору ресурсної політики. На відміну від підходів, у яких мультимодальне об'єднання даних і керування ресурсами розглядаються як незалежні задачі, запропонована концепція встановлює між ними безпосередній функціональний зв'язок. Це дає можливість розглядати ризик як проміжну характеристику стану системи, яка визначає необхідний рівень використання обчислювальних, комунікаційних та інших ресурсів.

Метою дослідження є розроблення методу інтелектуального ризик-орієнтованого аналізу мультимодальних багатовимірних даних, що забезпечує формування інтегрованої оцінки стану децентралізованої системи та використання отриманого рівня ризику для адаптивного розподілу її обмежених ресурсів. Досягнення поставленої мети передбачає розроблення способу узгодженого представлення різнорідних інформаційних потоків, визначення механізму адаптивної інтеграції модальних ознак, формування ризикової оцінки та встановлення її взаємозв'язку з процедурою ресурсного керування. Ефективність запропонованого підходу визначається за показниками якості інтелектуального аналізу, стійкості до неповноти інформації та ефективності використання ресурсів.

1 Постановка проблеми та аналіз існуючих підходів та публікацій

Проблема інтелектуального аналізу багатовимірних даних у сучасних розподілених системах набуває нового змісту внаслідок одночасної зміни характеру інформації, способів її отримання та умов прийняття рішень. Якщо у

класичних задачах МН припускається наявність відносно однорідного набору ознак, сформованого в єдиному інформаційному середовищі, то в сучасних децентралізованих системах дані формуються на різних вузлах, надходять із джерел різної природи та характеризуються неоднаковою часовою, просторовою і статистичною структурою. Це змінює вимоги до побудови інтелектуальних моделей. Виникає необхідність не тільки встановити закономірності в даних, а й визначити, наскільки інформація з окремого джерела є релевантною поточному стану системи, якою є її достовірність та як її використання має впливати на подальше рішення.

Одним із найбільш розвинених напрямів розв'язання цієї проблеми є мультимодальне МН, у межах якого декілька інформаційних модальностей використовуються для формування спільного представлення об'єкта або процесу. У ранніх роботах основна увага приділялася визначенню місця злиття даних у структурі моделі. Відповідно розглядалися рання інтеграція первинних ознак, проміжне об'єднання латентних представлень та пізнє злиття результатів окремих моделей. Така класифікація залишається корисною для аналізу архітектури, однак сучасний розвиток нейромережевих моделей істотно ускладнив межі між етапами вилучення ознак, їх інтеграції та формування кінцевого рішення. У сучасних системах ці операції можуть виконуватися спільно в межах єдиної параметризованої архітектури [16, 17].

Глибоке мультимодальне злиття даних продемонструвало здатність враховувати не тільки індивідуальні властивості модальностей, але й взаємозв'язки між ними. Аналіз ряду робіт [15, 16, 17] показує, що традиційні методи об'єднання не завжди здатні відтворювати складні міжмодальні залежності, тоді як нейромережеві представлення дозволяють формувати більш інформативний спільний простір ознак. Водночас автори відзначають наявність проблем, пов'язаних із неоднорідністю модальностей, складністю навчання та необхідністю врахування взаємодії між джерелами інформації [16]. Демонструється перехід до архітектур, заснованих на механізмах уваги, графових моделях, encoder-decoder структурах та великих попередньо навчених моделях. Це свідчить про те, що сама задача fusion уже не може бути зведена до конкатенації ознак або простого усереднення результатів [17].

Особливої уваги заслуговує питання нерівноцінності різних модальностей. У практичній системі інформаційні джерела не є стабільно еквівалентними. Один канал може мати високу точність у певному діапазоні станів, але втрачати інформативність за інших умов. Інший може містити значну кількість пропусків, шумів або запізнілих повідомлень. Тому використання постійних коефіцієнтів злиття є обмеженим рішенням. Навіть якщо оптимальні ваги визначено під час навчання, вони можуть перестати відповідати реальному розподілу інформаційної цінності під час експлуатації системи [18].

Додаткове ускладнення створює неповнота мультимодальної інформації. У реальних умовах відсутність певної модальності може бути наслідком відмови сенсора, порушення каналу зв'язку, обмеження енергоспоживання або відсутності відповідного джерела на конкретному вузлі. У результаті модель, яка навчалася на повному наборі модальностей, може демонструвати суттєве погіршення якості під час роботи з неповним інформаційним представленням.

Сучасні дослідження показують, що дана проблема охоплює пропуски, шум, дисбаланс та динамічну зміну якості окремих джерел. Отже, надійність системи мультимодального аналізу не може визначатися лише показниками, отриманими на повному та попередньо очищеному наборі даних [19].

Важливим напрямом розвитку мультимодальних моделей стали архітектури ГН на базі трансформерів. Їх застосування дозволило перейти від локального аналізу окремих ознак до моделювання складних залежностей між елементами різних інформаційних послідовностей [19]. Перевагою такого підходу є здатність моделі адаптивно визначати інформаційно значущі компоненти вхідних послідовностей. Разом із тим висока обчислювальна складність таких моделей обмежує можливість їх безпосереднього перенесення на периферійні вузли з обмеженими ресурсами. У децентралізованому середовищі виникає компроміс між якістю представлення даних та витратами на обчислення, пам'ять і передавання параметрів.

Інший перспективний напрям пов'язаний із використанням графових нейронних мереж. Для розподіленої мережі природним представленням системи є граф, вершини якого можуть відповідати обчислювальним або сенсорним вузлам, а ребра характеризувати комунікаційні зв'язки, залежності між джерелами або взаємодію інформаційних потоків. GNN-моделі дають можливість враховувати характеристики окремого вузла та контекст його взаємодії з іншими елементами мережі, що відрізняє графове представлення від традиційного табличного опису стану [20, 21]. Для задач, у яких необхідно приймати рішення в режимі, близькому до реального часу, виникає питання доцільності використання максимально складної архітектури. Якщо приріст точності супроводжується значним збільшенням часу оброблення, пам'яті або мережевого обміну, модель може виявитися непридатною для периферійного використання. Таким чином, у задачі децентралізованого аналізу необхідно оцінювати не тільки якість моделі, але й ціну отримання відповідної оцінки. Окремий клас методів утворюють моделі прогнозування фінансових ризиків. Фінансові дані є особливо складним об'єктом інтелектуального аналізу через нелінійність, часову залежність, зміну статистичних властивостей та взаємний вплив факторів. У дослідженнях фінансового ризику використовуються класичні методи статистичного аналізу, дерева рішень, ансамблеві алгоритми, нейронні мережі та гібридні моделі. Сучасні огляди показують поширення комбінацій моделей на базі CNN, LSTM та механізмів уваги для аналізу фінансових часових рядів [22]. Перевагою таких моделей є можливість одночасного вилучення локальних закономірностей та часових залежностей. Проте більшість робіт концентрується на підвищенні якості прогнозування конкретного фінансового показника або ризикового класу. Методологічна проблема полягає в тому, що ризикова оцінка у фінансовій задачі часто розглядається як кінцевий результат моделі. Додатковим фактором є необхідність інтерпретації ризикових рішень. Для фінансових систем це пов'язано з вимогами до довіри, контролю та можливості пояснення причин отриманого результату [23]. Для запропонованої проблематики це означає, що ризик-орієнтований механізм не повинен бути повністю відокремлений від інформаційних характеристик, на яких він базується.

Іншу групу становлять методи розподіленого навчання. Однією з принципових проблем децентралізованих мереж є те, що централізоване збирання всіх первинних даних не завжди можливе. Федеральне навчання запропонувало модель, у якій дані залишаються локально, а глобальна модель формується шляхом агрегування локальних оновлень, як це показано авторами на прикладі можливісті суттєвого скорочення комунікаційних витрат порівняно з синхронним централізованим навчанням [24]. Проте федеративне навчання не розв'язує автоматично проблему гетерогенності даних. Локальні вузли можуть мати різний обсяг інформації, неоднакові розподіли класів та різні набори модальностей. У такій ситуації однакова участь кожного вузла в агрегуванні може бути недостатньо обґрунтованою. Один вузол може мати доступ до часових рядів і сенсорної інформації, інший може містити тільки структуровані характеристики, а третій може характеризуватися обмеженою якістю даних. Це створює передумови для поєднання адаптивного fusion із механізмами розподіленого навчання.

Паралельно розвиваються методи інтелектуального керування ресурсами в edge та IoT-середовищах. Зокрема у [25] розглянуто використання ГН з підкріпленням для задач обчислювального характеру у edge секторі [25]. Автори виходять із того, що складний і динамічний стан мережі ускладнює застосування традиційних методів оптимізації. Аналогічні підходи використовуються для спільного вирішення задач offloading та розподілу ресурсів у спеціалізованих edge-середовищах [26]. Перевагою такого підходу є здатність адаптувати політику до динамічної зміни стану системи. Однак стан середовища зазвичай задається параметрами навантаження, доступності каналів, обчислювальної потужності, енергетичного запасу та інших мережевих характеристик. Інформаційний ризик як окрема складова стану найчастіше не розглядається, унаслідок цього алгоритм може оптимально розподіляти ресурси з точки зору затримки або енергоспоживання, але не враховувати критичність завдання. Ще одним обмеженням традиційних моделей ресурсного керування є їхня орієнтація на поточний стан мережі. У такому разі рішення формується на основі доступних у цей момент ресурсів, а не прогнозованого розвитку стану. Поєднання різних підходів до аналізу даних дозволяє частково усунути цю проблему, оскільки прогноз може використовуватися для попереднього визначення майбутнього навантаження або вибору оптимального місця виконання завдання [27]. Однак і тут прогнозний модуль та модуль керування зазвичай залишаються функціонально розділеними. Необхідність інтегрувати прогнозований ризик, якість інформації та ресурсний стан у єдину модель прийняття рішення залишається актуальною.

Значний інтерес становлять також багатоагентні та розподілені підходи. Вони дозволяють декільком вузлам самостійно приймати рішення, координуючи свої дії через обмін інформацією. Такий механізм краще відповідає структурі децентралізованої мережі, ніж централізований контролер, оскільки зменшує залежність системи від єдиного вузла прийняття рішень. Разом із тим зростання кількості агентів збільшує простір можливих станів і дій, а отже, ускладнює процес навчання. Крім того, кожен агент може мати лише часткове спостереження за глобальним станом мережі. У таких умовах

якість локального рішення залежить від того, наскільки правильно інтегровано локальну інформацію з інформацією, отриманою від інших вузлів. Узагальнення результатів аналізу дозволяє виділити декілька принципових обмежень існуючих підходів. По-перше, більшість мультимодальних моделей оптимізується за кінцевою якістю прогнозування і недостатньо враховує вартість оброблення. По-друге, фінансові ризикові моделі зазвичай завершуються формуванням прогнозної оцінки та не використовують її як безпосередній параметр керування ресурсами. По-третє, методи ресурсного керування переважно працюють із технічними параметрами мережі та не враховують інформаційну критичність завдань. По-четверте, федеративне навчання забезпечує локальність даних, але не гарантує адекватного врахування неоднакової інформаційної цінності вузлів і модальностей. По-п'яте, складні нейромережеві архітектури можуть бути непридатними для периферійної реалізації без спеціального механізму адаптації обчислювального навантаження. Аналітичне порівняння існуючих підходів наведено в таблиці 1. Порівняння показує, що найбільш перспективним напрямом є функціональне поєднання переваг різних алгоритмів. Мультимодальні моделі доцільно використовувати для формування інформаційно насиченого представлення, часові моделі для врахування динаміки, графові моделі для опису взаємозалежностей між вузлами, а гібридні моделі ГН з підкріпленням для адаптивного вибору дій. При цьому необхідно запровадити проміжну ризикову характеристику, яка пов'язує результати інтелектуального аналізу з ресурсною політикою. З урахуванням проведеного аналізу пропонується розглядати ризик як інтегральний стан, що формується на основі декількох інформаційних модальностей і визначає пріоритетність подальшого використання ресурсів. Відповідно, наукова проблема полягає у необхідності розроблення такого способу інтеграції МАД, за якого різні джерела інформації враховуються з урахуванням їх поточної інформативності та невизначеності, а сформована ризикова оцінка використовується не лише для прогнозування небажаних станів, а й для адаптивного керування обмеженими ресурсами децентралізованої мережі. Отже, аналіз наукових публікацій підтверджує наявність достатньої теоретичної основи для окремого використання мультимодального ГН, фінансового ризик-аналізу, графового моделювання, федеративного навчання та інтелектуального керування ресурсами. Водночас їх роздільне застосування не забезпечує повного розв'язання задачі, у якій інформаційна неоднорідність, ризик та ресурсні обмеження взаємно впливають один на одного. Саме ця невідповідність визначає доцільність розроблення інтегрованого ризик-орієнтованого методу, що поєднує адаптивну мультимодальну інтеграцію даних із механізмом формування та використання ризикової оцінки для керування ресурсами децентралізованої мережі. Подальший розвиток дослідження пов'язаний із формалізацією такої моделі та визначенням математичних залежностей між інформаційним станом, рівнем ризику та ресурсною політикою.

Таблиця 1.

Аналітичне порівняння існуючих підходів

Підхід	Основний принцип	Сильна сторона	Ключове обмеження	Перспектива інтеграції
Мульти-модальне глибинне злиття	Спільне представлення різних модаль-ностей	Врахування взаємодо-повнювальної інформації	Чутливість до пропусків, шуму	Адаптивне зважування за якістю та ризиком
Гібридне прогно-зування часових рядів	Поєднання CNN, LSTM, Transformer та уваги	Виявлення просторових і часових залежностей	Орієнтація переважно на точність прогнозу	Передавання прогно-зованого ризику в контур керування
Графове інтелек-туальне моделю-вання	Представлення вузлів та їх взаємодій графом	Урахування структурних залежностей мережі	Висока складність та складне врахування якості даних	Поєднання GNN з multimodal fusion та risk assessment
DRL для керування ресурсами	Навчання політики на базі стану, винагороди	Адаптивність до динаміки мережі	Ризик часто не входить до стану та функції винагороди	Формування risk-aware політики розподілу ресурсів

2 Формалізація та розробка запропонованого методу

Запропонований у роботі метод спрямований на побудову єдиного аналітико-керуючого підходу, у якому мультимодальні дані, що надходять від децентралізованих вузлів, інтегруються з урахуванням їх поточної інформаційної цінності, після чого на основі сформованого представлення визначається ризиковий стан та приймається рішення щодо розподілу доступних ресурсів. Така постановка відрізняється від послідовного застосування незалежних моделей тим, що результат інтелектуального аналізу безпосередньо впливає на подальший режим функціонування системи. При цьому ресурсні обмеження також розглядаються як фактор, що визначає можливості оброблення інформації та, відповідно, повноту аналітичного представлення. У запропонованій моделі децентралізована мережа розглядається як множина взаємодіючих вузлів, кожен із яких у певний момент часу може отримувати декілька типів інформації. Така інформація може характеризувати фінансові операції, ринкові показники, поведінкові характеристики, часові послідовності, технічний стан вузла або параметри мережевої взаємодії. Залежно від предметної області конкретний склад модальностей може змінюватися, однак принцип їх спільного аналізу залишається незмінним.

2.1.1 Модель мультимодального спостереження та оцінювання якості даних

Нехай децентралізована мережа містить N вузлів, а на кожному вузлі доступні M інформаційних модальностей. Сукупність спостережень, доступних на вузлі i у момент часу t, подамо у вигляді

$$X_i^{(t)} = \{x_{i,1}^{(t)}, x_{i,2}^{(t)}, ..., x_{i,M}^{(t)}\}\ , \quad (1)$$

де $X_i^{(t)}$ – повна множина мультимодальних спостережень на вузлі i у момент часу t, $x_{i,M}^{(t)}$ – дані m -ї модальності на вузлі i у момент часу t.

Принциповим для подальшої обробки є те, що наявність даних не означає однакову інформативність кожного джерела. На практиці якість окремої модальності може змінюватися через шум, пропуски, затримки передавання, нестабільність сенсорного обладнання або зміну характеру процесу, що спостерігається. Тому перед інтеграцією даних необхідно визначити поточну якість кожного інформаційного потоку. Для цього кожній модальності ставиться у відповідність нормований показник якості $q_{i,m}^{(t)}$, значення якого належить інтервалу від 0 до 1. Нульове значення відповідає ситуації, коли інформація практично непридатна для поточного аналізу, тоді як значення, близьке до одиниці, характеризує високий рівень її достовірності та повноти. На основі цього показника формується адаптивна вага модальності

$$w_{i,m}^{(t)} = \frac{\exp(\alpha q_{i,m}^{(t)})}{\sum_{k=1}^{M} \exp(\alpha q_{i,k}^{(t)})}\ , \quad (2)$$

де $w_{i,m}^{(t)}$ – нормована вага m-ї модальності на вузлі i у момент часу t, $q_{i,m}^{(t)}$ – оцінка якості m-ї модальності, α - параметр чутливості механізму зважування до зміни якості інформації, k - індекс модальності, за якою виконується нормування. Використання експоненційного нормування дозволяє уникнути жорсткого відсікання інформаційних джерел. Навіть модальність із відносно низькою якістю не вилучається автоматично, а зменшує свій вплив на інтегроване представлення. Це важливо для децентралізованої мережі, оскільки тимчасове погіршення одного каналу не повинно призводити до повної втрати відповідного інформаційного напряму. Параметр α визначає, наскільки швидко змінюється співвідношення між вагами при зміні якості. За невеликих значень цього параметра система поводиться більш толерантно до відмінностей між модальностями, його збільшення посилює вплив найбільш якісного джерела. Визначення показника $q_{i,m}^{(t)}$ може виконуватися на основі сукупності характеристик, серед яких доцільно враховувати частку пропущених значень, рівень шуму, часову актуальність, стабільність передавання та узгодженість інформації з іншими доступними джерелами. Важливо, що сам механізм оцінювання якості не повинен бути жорстко прив'язаний до конкретної предметної області. Це забезпечує можливість використання методу як для фінансових потоків, так і для сенсорної або мережевої інформації.

2.2 Адаптивне злиття модальностей та формування інтегрованого представлення

Після оцінювання якості кожен інформаційний потік обробляється окремим модальним енкодером, через те, що структура різних типів даних може суттєво

відрізнятися. Для часових послідовностей доцільними є моделі, здатні враховувати залежності між попередніми та поточними станами. Для структурованих даних можуть використовуватися багатошарові перцептрони або інші моделі табличного представлення. У випадку графової структури мережі доцільним є використання графового енкодера, який враховує взаємодію вузлів. Гібридність запропонованого методу реалізується через функціональний розподіл ролей між різними моделями оброблення. Для кожної модальності формується латентне представлення

$$z_{i,m}^{(t)} = f_m(x_{i,m}^{(t)}; \theta_m), \quad z_{i,m}^{(t)} \mathfrak{R}^d, \tag{3}$$

де $z_{i,m}^{(t)}$ – латентне представлення *m*-ї модальності на вузлі *i* у момент часу *t*, f_m – функція енкодера відповідної модальності, $x_{i,m}^{(t)}$ – вихідні дані модальності, θ_m – параметри енкодера, *d* – розмірність спільного латентного простору.

Приведення модальних представлень до єдиного латентного простору є необхідною умовою їх подальшого порівняння та інтеграції. При цьому конкретна архітектура може відрізнятися для різних модальностей. Наприклад, часовий потік може оброблятися LSTM або Transformer, локальні числові характеристики - MLP, а структурні залежності між вузлами — GNN. Важливим є не використання певної моделі як такої, а забезпечення спільної розмірності представлень, що дозволяє виконати їх адаптивне злиття.

Інтегроване представлення вузла формується як зважена комбінація латентних представлень

$$z_i^{(t)} = \sum_{m=1}^{M} w_{i,m}^{(t)} z_{i,m}^{(t)}, \tag{4}$$

де $z_i^{(t)}$ – інтегроване латентне представлення стану вузла *i* у момент часу *t*, $w_{i,m}^{(t)}$ – адаптивна вага *m*-ї модальності, $z_{i,m}^{(t)}$ – латентне представлення відповідної модальності.

На відміну від простого об'єднання ознак конкатенацією, запропонований механізм дозволяє врахувати поточну інформаційну цінність джерел. У цьому випадку інтегроване представлення є динамічною характеристикою, яка змінюється не тільки під впливом самих даних, але й залежно від їх якості. Якщо, наприклад, один із потоків характеризується значною кількістю пропусків або втратою актуальності, його вага автоматично зменшується. Водночас інші модальності отримують більший відносний вплив на спільне представлення. Такий механізм особливо важливий у децентралізованих мережах, оскільки якість інформації на різних вузлах може відрізнятися. Один вузол може мати повний набір даних і достатню обчислювальну потужність, тоді як інший працюватиме з обмеженою кількістю модальностей. Метод не вимагає, щоб інформаційна структура всіх вузлів була повністю ідентичною. Зміна складу доступних даних відображається через значення показників якості та відповідне перерозподілення ваг. Слід підкреслити, що адаптивне злиття не виключає можливості використання механізмів уваги, які можуть бути

реалізовані всередині енкодерів або як додатковий механізм визначення інформаційної значущості. У запропонованій концепції показник $q_{i,m}^{(t)}$ виконує функцію зовнішнього щодо латентного простору індикатора якості, а внутрішні механізми уваги можуть визначати важливість окремих ознак або фрагментів послідовності.

Оцінювання ризикового стану

Сформоване інтегроване представлення використовується для визначення ризикового стану. У межах запропонованого методу ризик трактується як узагальнена характеристика ймовірності небажаного розвитку процесу або переходу системи до стану, що потребує підвищеної уваги з боку механізму керування. Ризиковий показник визначається за допомогою окремого модуля оцінювання

$$R_i^{(t)} = q(z_i^{(t)}; \theta_R), \quad R_i^{(t)} \in [0,1], \tag{5}$$

де $R_i^{(t)}$ – нормований показник ризику на вузлі *i* у момент часу *t*, q - функція оцінювання ризику, θ_R - параметри ризикової моделі, $z_i^{(t)}$ - інтегроване латентне представлення вузла.

Конкретна реалізація функції q залежить від постановки експерименту. Для задач класифікації вона може бути реалізована як вихід нейромережевого класифікатора, для прогнозування - як перетворення прогнозованої ймовірності небажаної події, а для багатофакторного аналізу — як регресійна модель ризикового індексу. Результат повинен мати узгоджену шкалу, яка дозволяє передавати його в модуль керування незалежно від конкретного типу вихідних даних. Ризикова оцінка в запропонованій системі не є самодостатнім результатом. Її основне призначення полягає у визначенні пріоритетності подальшого використання ресурсів. Це означає, що однакові технічні умови можуть приводити до різних керуючих дій залежно від критичності інформаційного процесу. Така властивість дозволяє сформувати risk-aware підхід до керування, за якого ресурси розподіляються не тільки відповідно до навантаження, а й відповідно до потенційних наслідків недостатнього рівня оброблення.

Ризик-орієнтоване керування ресурсами

На заключному етапі інтегроване представлення та оцінка ризику поєднуються з поточним ресурсним станом вузла. Під ресурсами розуміються обчислювальна потужність, оперативна пам'ять, енергетичний запас, пропускна здатність каналів зв'язку та інші характеристики, що визначають можливість виконання аналітичних і мережевих операцій.

Керуюче рішення формується параметризованою політикою

$$A_i^{(t)} = \pi_\theta(S_i^{(t)}, R_i^{(t)}, z_i^{(t)}), \tag{6}$$

де $A_i^{(t)}$ - керуюча дія щодо ресурсів на вузлі *i* у момент часу *t*, π_θ - параметризована політика керування, $S_i^{(t)}$ - поточний вектор доступних ресурсів вузла.

Функція π_θ може реалізовуватися різними способами залежно від вимог до системи. Для відносно простих задач можливе використання правил або оптимізаційного механізму. Для динамічного середовища, у якому послідовність рішень впливає на майбутній стан мережі, доцільним є використання reinforcement learning. У такому разі поточний ризик входить до стану агента, а якість ресурсного рішення визначається не тільки поточною затримкою або енергоспоживанням, а й наслідками недостатнього обслуговування критичного інформаційного потоку.

Принциповою особливістю моделі є наявність зворотного зв'язку. Зміна ресурсного стану впливає на доступність та якість інформаційних потоків, що в подальшому змінює оцінки $q_{i,m}^{(t)}$, адаптивні ваги модальностей та інтегроване представлення. За нормального стану мережі та низького ризику система може підтримувати стандартний рівень оброблення інформації. При зростанні ризику пріоритет критичного потоку підвищується, що може супроводжуватися збільшенням частоти аналізу, виділенням додаткових обчислювальних ресурсів або зміною маршруту передавання. Якщо одночасно погіршується якість одного з джерел, його внесок до інтегрованого представлення зменшується, а рішення приймається на основі доступних альтернативних модальностей. Саме така взаємодія забезпечує стійкість методу до зміни інформаційного та ресурсного стану. Отже, запропонований метод об'єднує чотири функціональні рівні. Перший забезпечує формування мультимодального спостереження та оцінювання якості інформації. Другий перетворює різнорідні дані в узгоджений латентний простір і виконує адаптивне злиття. Третій формує ризикову оцінку на основі інтегрованого стану. Четвертий використовує цю оцінку разом із поточним ресурсним станом для формування керуючої дії. Загальна схема реалізації підходу наведена на рис.1.



Рисунок 1. Загальна схема реалізації запропонованого підходу

Схема відображає послідовність функціонування методу від надходження різнорідних даних на децентралізовані вузли до формування керуючої дії. На першому рівні показано джерела мультимодальної інформації, фінансові,

поведінкові, часові та технічні дані. Далі кожен інформаційний потік проходить оцінювання якості та модальне кодування, після чого латентні представлення об'єднуються за адаптивними вагами. Сформований інтегрований стан передається до модуля оцінювання ризику, а результат разом із поточним ресурсним станом надходить до політики керування. Нижня частина схеми містить зворотний зв'язок, який показує вплив прийнятого рішення на подальшу доступність ресурсів, якість інформації та стан системи. Гібридний fusion-модуль (рис.2) реалізує послідовне перетворення різнорідних інформаційних потоків у єдине латентне представлення стану вузла. Спочатку для кожної модальності визначається показник якості, після чого на його основі встановлюється адаптивна вага інформаційного потоку. Далі використовуються спеціалізовані енкодери, які враховують природу відповідних даних, а отримані латентні представлення об'єднуються за схемою fusion-зважування. На виході формується узгоджене представлення та передається до модуля оцінювання ризику.



Рисунок 2. Гібридний fusion-модуль

Схема функціонального зв'язку між результатом мультимодального аналізу та керуванням ресурсами мережі наведена на рис.3. Вона показує функціональний зв'язок між результатом мультимодального аналізу та подальшим керуванням ресурсами мережі. Інтегроване представлення використовується для визначення рівня ризику, який разом із поточним станом ресурсів визначає керуючу дію. Реалізація цієї дії змінює обчислювальний, енергетичний та комунікаційний стан вузла, а також може впливати на якість інформації, що надходить у наступному часовому циклі. Зворотний зв'язок забезпечує адаптацію системи до зміни умов функціонування та перетворює окреме рішення щодо ресурсів на безперервний процес інтелектуального керування.



Рисунок 3. Схема функціонального зв'язку між результатом мультимодального аналізу та керуванням ресурсами мережі

3 Дослідження роботи та обчислювальні експерименти

Експериментальні дослідження були спрямовані на перевірку здатності запропонованого методу забезпечувати одночасне підвищення якості ризикового аналізу та ефективності використання обмежених ресурсів децентралізованої мережі. Основна увага приділялася абсолютному значенню показників класифікації та характеру зміни результатів за умов погіршення інформаційної якості та зростання ресурсного навантаження. Така постановка дає змогу перевірити основну гіпотезу роботи, відповідно до якої поєднання адаптивного мультимодального злиття з ризик-орієнтованим керуванням та повинно забезпечувати більш стійку поведінку системи порівняно з моделями, у яких аналіз даних та ресурсне керування виконуються незалежно.

Експериментальний стенд реалізовано на основі програмної архітектури Python із використанням середовища Jupyter Notebook, бібліотек NumPy та Pandas для підготовки і трансформації даних, Scikit-learn для побудови базових моделей та обчислення статистичних характеристик, PyTorch для реалізації глибинних компонентів запропонованого підходу, а також Matplotlib для формування графічного представлення результатів. Архітектура відповідає структурі розробленого методу та включає рівні завантаження і попередньої обробки мультимодальних даних, формування модальних представлень, адаптивного злиття, оцінювання ризику та прийняття відповідних аналітичних рішень. Обчислювальна реалізація передбачає можливість незалежної обробки окремих модальностей із подальшим передаванням їх латентних представлень до спільного fusion-рівня, що дає змогу моделювати ситуації неповноти, різної якості та неоднорідності вхідної інформації. Для формування вхідного інформаційного середовища використано відкриті набори даних, які характеризуються різною природою ознак та часовою структурою. Основним джерелом для експериментів обрано відкритий набір IEEE-CIS Fraud Detection [26]. Його структура безпосередньо відповідає концепції мультимодального фінансового аналізу, оскільки дані розділені на транзакційну таблицю та таблицю ідентифікаційних і пристроєвих характеристик, які пов'язуються за ідентифікатором TransactionID. Навчальна частина містить 590 540 транзакційних записів із 394 полями та 144 233 записи ідентифікаційної інформації з 41 полем, причому додаткові identity-ознаки доступні лише для частини транзакцій. Транзакційна модальність містить інформацію про суму операції, часову характеристику, тип продукту, платіжні та агреговані

статистичні ознаки, тоді як identity-модальність характеризує пристрій, браузер, операційну систему та інші анонімізовані параметри цифрового середовища здійснення операції.

Зазначена структура є важливою для досліджуваного методу, оскільки дозволяє розглядати окремі групи ознак як незалежні інформаційні модальності та досліджувати вплив їх доступності й якості на оцінку ризику. При цьому приблизно 24,4 % навчальних транзакцій мають відповідний identity-запис, тоді як для решти операцій така інформація відсутня, що створює природне середовище для перевірки механізму адаптивного зважування модальностей та його поведінки за неповної інформації. Саме ця властивість набору IEEE-CIS робить його більш придатним для перевірки запропонованої архітектури, ніж набори, у яких усі ознаки представлені однорідною таблицею. Для додаткового представлення часової та поведінкової складової використано набір UCI Online Retail [27], який містить 541 909 транзакцій онлайн-роздрібного бізнесу за період від 1 грудня 2010 року до 9 грудня 2011 року. Кожний запис характеризується ідентифікатором рахунку, кодом товару, описом продукції, кількістю, датою і часом операції, ціною одиниці продукції, ідентифікатором клієнта та країною. Набір містить 4 372 ідентифікованих клієнти, а його послідовний характер дозволяє оцінювати не тільки окрему операцію, а й зміну поведінкового профілю в часі.

Окрему незалежну вибірку для перевірки узагальнювальної здатності ризикового компонента сформовано на основі набору UCI Default of Credit Card Clients [28]. Перед подаванням даних до моделей виконано уніфікацію форматів, очищення пропусків, кодування категоріальних ознак, масштабування числових характеристик та формування часових і поведінкових агрегатів. Транзакційні дані об'єднувалися за TransactionID, відсутність відповідної identity-інформації не розглядалася як причина автоматичного вилучення транзакції, оскільки саме неповнота однієї з модальностей є одним із досліджуваних факторів. Також на рівні клієнта формувалися послідовності операцій та агреговані характеристики активності та зберігалася початкова клієнтська структура з подальшим нормуванням числових ознак і кодуванням дискретних змінних. У результаті вхідне інформаційне середовище експериментального стенда охоплює транзакційні, поведінкові, часові, клієнтські та цифрові ідентифікаційні характеристики, що відповідає вимогам до мультимодального ризик-орієнтованого аналізу.

Для проведення порівняльного експерименту сформовано середовище, у якому інформаційний стан вузла описується чотирма взаємодоповнювальними модальностями. До першої групи віднесено часові характеристики процесу, до другої структуровані числові параметри, до третьої характеристики взаємодії вузлів мережі, до четвертої агреговані показники поточного ресурсного та інформаційного стану. Такий склад дозволяє одночасно перевірити можливість оброблення різнорідних даних і врахування мережевого контексту під час формування ризикової оцінки.

У базовому експериментальному сценарії розглядалася ситуація, у якій частина інформаційних потоків характеризується змінною якістю. Для окремих фрагментів даних моделювалися пропуски, шумові спотворення та зниження

актуальності інформації. Одночасно змінювався рівень завантаження обчислювальних і комунікаційних ресурсів. Для порівняння використовувалися чотири варіанти побудови системи. Перший варіант передбачав раннє злиття, за якого первинні ознаки різних модальностей об'єднувалися до передачі в єдину модель. Другий варіант реалізував пізнє злиття, коли кожна модальність аналізувалася окремо, а кінцеві результати об'єднувалися на виході. Третій варіант використовував статичне зважування модальностей, коефіцієнти їх внеску не змінювалися протягом експерименту. Четвертий варіант відповідав запропонованому методу, у якому вага інформаційного потоку визначалася адаптивно, а сформований ризиковий показник додатково використовувався для керування ресурсами.

Для оцінювання якості ризикового аналізу застосовувалися F1-міра та ROC-AUC [29]. Для оцінювання практичної ефективності використовувалися середня затримка оброблення одного запиту та енерговитрати на його виконання. Отримані результати наведено в табл. 2.

Таблиця 2

Порівняльні результати експериментального дослідження

Метод	F1	ROC-AUC	Середня затримка, мс	Енерговитрати, Дж/задачу
Раннє злиття	0,861	0,913	42,6	1,84
Пізнє злиття	0,874	0,926	46,8	2,02
Статичне зважене злиття	0,891	0,944	44,1	1,91
Запропонований метод	0,927	0,968	39,2	1,63

Наведені результати свідчать, що запропонований метод забезпечує найкращі значення за всіма чотирма критеріями. F1-міра досягає 0,927, тоді як для раннього злиття вона становить 0,861, для пізнього 0,874, а для статичного зваженого злиття 0,891. Отже, порівняно зі статичним зважуванням приріст F1 становить 0,036 абсолютного значення, або близько 4,0 %. Відносно раннього злиття покращення становить близько 7,7 %, а порівняно з пізнім злиттям близько 6,1 %. Зростання F1 не є наслідком простого збільшення складності моделі. Важливішим фактором є адаптивний характер запропонованого fusion-механізму. У ранній схемі злиття шумова або неповна модальність потрапляє безпосередньо в загальний простір ознак і може впливати на всі подальші етапи. При пізньому злитті проблема частково послаблюється завдяки незалежному аналізу модальностей, кінцевий механізм не має достатньої інформації про те, наскільки достовірним було кожне джерело в конкретний момент. Статичне зважування усуває частину цього недоліку, не враховуючи динамічної зміни якості даних. Запропонований метод змінює вагу модальності відповідно до її поточного стану, тому деградований канал не має такого самого впливу, як повноцінне інформаційне джерело. ROC-AUC запропонованого методу становить 0,968. Для статичного зваженого злиття отримано 0,944, тобто приріст дорівнює приблизно 2,5 %. Порівняно з раннім злиттям приріст становить близько 6,0 %. Це підтверджує, що адаптивне зважування впливає не тільки на окремі порогові рішення, а й на загальну здатність системи розділяти нормальні та ризикові стани. Важливою характеристикою є також зниження

обчислювальної затримки. Для запропонованого методу середня затримка становить 39,2 мс, тоді як для статичного зваженого злиття вона дорівнює 44,1 мс. Таким чином, час оброблення скорочується приблизно на 11,1 %. Порівняно з пізнім злиттям зменшення становить близько 16,2 %, а порівняно з раннім злиттям близько 8,0 %. За зниження якості або низької критичності окремого джерела його внесок зменшується, що скорочує непотрібне обчислювальне та комунікаційне навантаження. Подібна тенденція спостерігається для енерговитрат. Запропонований метод потребує в середньому 1,63 Дж на одну оброблену задачу, тоді як статичне зважене злиття потребує 1,91 Дж. Отже, економія становить близько 14,7 %. Порівняно з раннім злиттям зменшення енерговитрат становить приблизно 11,4 %, а порівняно з пізнім злиттям 19,3 %. Рішення щодо виділення ресурсу пов'язується з оціненим ризиком, тому додаткові обчислювальні витрати концентруються на тих процесах, для яких помилка або затримка можуть мати більші наслідки. Результати порівняння якості ризикової класифікації графічно подано на рис. 4.

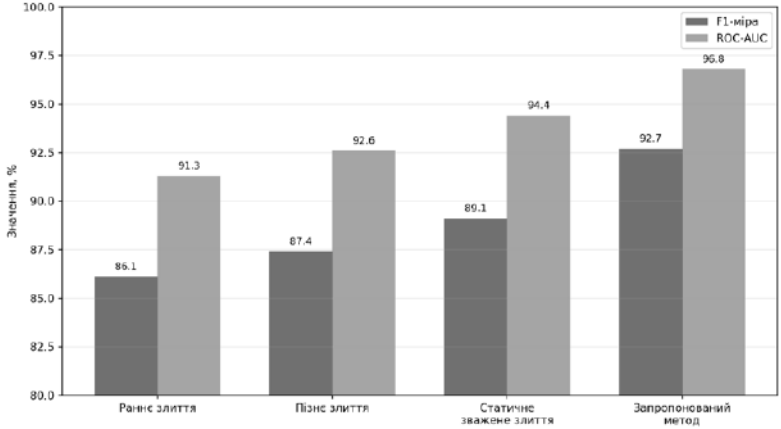


Рисунок 4. Порівняння якості ризикової класифікації

Дана візуалізація показує, що запропонований метод має перевагу одночасно за F1 та ROC-AUC, тобто покращення не обмежується одним критерієм. Найбільший ефект спостерігається порівняно з раннім злиттям, яке виявляється найбільш чутливим до неоднорідності первинних ознак. Перевага над статичним зважуванням є меншою, але саме вона демонструє внесок адаптивної складової запропонованої архітектури. Наступним етапом було дослідження поведінки моделей за зміни ресурсного навантаження. Навантаження змінювалося від 30 до 95 %, що дозволило перевірити стійкість системи в умовах наближення до дефіциту обчислювальних ресурсів. У цьому експерименті особливо важливим є швидкість її зростання при переході до перевантаженого стану. За навантаження 30 % різниця між методами є незначною. Середня затримка запропонованого методу становить 31,4 мс проти 33,2 мс для статичного зваженого злиття. При збільшенні навантаження до 70 % різниця зростає до 7,8 мс, оскільки запропонована модель починає активніше

використовувати інформацію про ризик під час розподілу ресурсів. При навантаженні 95 % затримка запропонованого методу становить 49,6 мс, тоді як для статичного підходу вона збільшується до 69,4 мс. Особливе значення має форма кривих зростання ресурсного навантаження, що наведені на рис. 5.

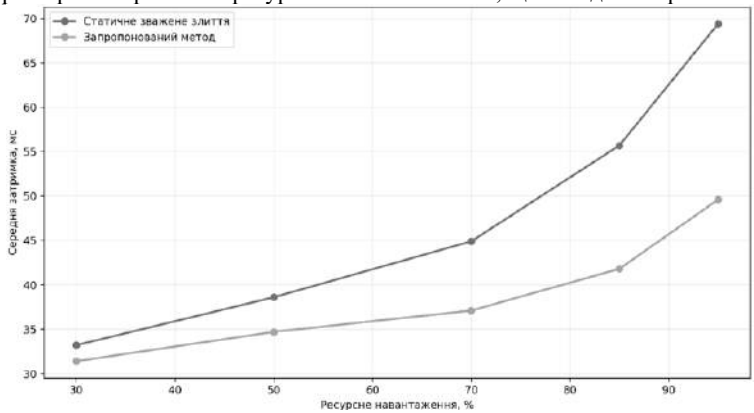


Рисунок 5. Стійкість зростання ресурсного навантаження

Для статичного підходу після перевищення 70 % навантаження спостерігається прискорене збільшення затримки. Це означає, що статична схема не встигає адаптуватися до дефіциту ресурсів, а запропонований метод демонструє більш плавне зростання затримки, оскільки ризиковий контур дозволяє динамічно змінювати пріоритети та не витрачати однаковий обсяг ресурсів на всі інформаційні потоки. Для визначення внеску окремих компонентів запропонованої архітектури проведено абляційний експеримент. У повній моделі одночасно використовувалися адаптивне зважування, ризик-орієнтований контур та графовий контекст. Далі кожен із цих компонентів по черзі вилучався при збереженні інших параметрів без змін. Результати наведено на рис. 6. Повна модель забезпечує F1 на рівні 0,927. Вилучення адаптивного механізму зважування знижує цей показник до 0,901, тобто приблизно на 2,8 %. Відмова від ризик-орієнтованого контуру призводить до найбільшого погіршення - F1 зменшується до 0,884, що відповідає втраті близько 4,6 % відносно повної моделі. Вилучення графового контексту знижує F1 до 0,909, тобто приблизно на 1,9 %. Отримане співвідношення є важливим для інтерпретації результатів, оскільки показує, що найбільший внесок у загальну якість має зв'язок між ризиковою оцінкою та механізмом адаптивного керування. Якщо прибрати адаптивні ваги, якість моделі зменшується з 0,927 до 0,901. Отже, приблизно третина від різниці між запропонованим методом і простішими схемами злиття пов'язана з можливістю враховувати поточну якість модальностей. Водночас більш суттєве падіння при вилученні ризикового контуру свідчить, що перевага методу визначається не тільки якістю інформаційного представлення. Важливу роль відіграє використання отриманої аналітичної інформації для подальшого керування системою.

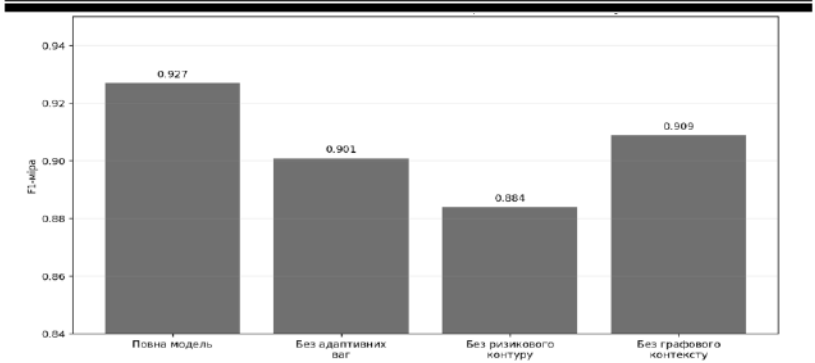


Рисунок 6. Абляційний аналіз компонентів запропонованого методу

Узагальнюючи результати, можна стверджувати, що запропонована модель демонструє перевагу за двома взаємопов'язаними групами критеріїв. Перша група характеризує якість інтелектуального аналізу, а друга група характеризує експлуатаційну ефективність. Основна причина отриманої переваги полягає у функціональному поєднанні трьох механізмів: адаптивний fusion зменшує вплив ненадійних модальностей, інтегральна оцінка ризику визначає пріоритетність інформаційних процесів, а замкнений ресурсний контур адаптує обчислювальні та комунікаційні ресурси до поточної критичності задач. Такий результат узгоджується із сучасною тенденцією переходу від статичних алгоритмів розподілу ресурсів до адаптивних методів, у яких стан мережі та характеристики задачі використовуються для формування поточної політики керування. Зокрема, сучасні роботи з DRL для edge/IoT-середовищ показують переваги адаптивного врахування затримки, енергоспоживання та стану ресурсів. Проведене дослідження підтверджує доцільність використання гібридної архітектури для задач, у яких одночасно необхідно аналізувати різнорідні багатовимірні дані та керувати обмеженими ресурсами. Експеримент показав, що просте збільшення кількості модальностей або використання складнішої нейромережевої моделі не забезпечує такого ефекту без механізму адаптивного визначення їхньої інформаційної цінності. Найбільша перевага виникає тоді, коли результати інтелектуального аналізу включаються безпосередньо в контур керування.

Отже, результати експериментальних досліджень підтверджують сформульовану в роботі гіпотезу про доцільність інтеграції мультимодального аналізу, оцінювання ризику та адаптивного ресурсного керування. Запропонований метод забезпечує підвищення якості ризикової класифікації на 4,0 % порівняно зі статичним зваженим злиттям, зменшення середньої затримки на 11,1 % та скорочення енерговитрат приблизно на 14,7 %. За високого ресурсного навантаження перевага за затримкою зростає до 28,5 %, що свідчить про ефективність запропонованого підходу саме в умовах дефіциту ресурсів. Це дає підстави розглядати розроблений метод як основу для побудови адаптивних інтелектуальних систем, у яких якість аналізу даних та

ефективність використання ресурсів визначаються в межах єдиного замкненого контуру.

Висновки

У результаті проведеного дослідження розроблено метод інтелектуального ризик-орієнтованого аналізу мультимодальних багатовимірних даних для адаптивного керування ресурсами децентралізованих мереж, який поєднує засоби глибинного представлення неоднорідної інформації, адаптивного мультимодального злиття, оцінювання ризикового стану та формування керувальних рішень щодо розподілу обмежених обчислювальних, комунікаційних та енергетичних ресурсів. На відміну від підходів, у яких аналіз інформації та керування ресурсами розглядаються як відокремлені етапи, запропонований метод формує замкнену функціональну взаємодію між якістю вхідних даних, рівнем оціненого ризику, поточним станом ресурсів та наступною стратегією їх використання. Це дозволяє розглядати мультимодальність як механізм формування адаптивного інформаційного середовища, здатного змінювати власну структуру відповідно до поточних умов функціонування мережі.

Основною методологічною особливістю запропонованого рішення є розподіл процесу інтелектуального аналізу на взаємопов'язані рівні, кожний з яких виконує окрему функціональну роль. Первинні інформаційні потоки проходять модально-специфічне кодування, унаслідок чого різнорідні транзакційні, часові, поведінкові, клієнтські та цифрові характеристики переводяться у зіставний латентний простір. Подальше адаптивне злиття здійснюється з урахуванням поточної якості кожної модальності, що принципово відрізняє запропонований підхід від статичних схем комбінування ознак. У ситуації, коли окремий інформаційний канал характеризується пропусками, шумом, затримкою або зниженням достовірності, його внесок у сформоване представлення може бути автоматично зменшений, тоді як більш інформативні модальності отримують вищу вагу. Завдяки цьому інтегроване представлення ризикового стану стає менш залежним від стабільності окремого джерела інформації. Важливим результатом є встановлена взаємозалежність між якістю прогнозування та ресурсною ефективністю. Запропонований метод продемонстрував найменшу серед досліджених підходів затримку обробки, яка у модельному експерименті становила 39,2 мс проти 44,1 мс для статичного зваженого злиття. Зниження затримки становить близько 11,1 %. Порівняно з раннім злиттям скорочення становить близько 8,0 %, а відносно пізнього злиття досягає 16,2 %. Важливою особливістю запропонованого методу є його орієнтація на функціонування в децентралізованих мережах, де централізована передача всього обсягу первинних даних до єдиного обчислювального вузла може бути неефективною або недоцільною. Модульна організація архітектури створює можливість локального опрацювання окремих потоків із передаванням у спільний простір лише компактних латентних представлень, оцінок їх якості або ризикових характеристик. Це потенційно зменшує обсяг мережевого обміну та дозволяє масштабувати запропоновану концепцію на системи з неоднорідними вузлами та різними рівнями обчислювальної спроможності. Практичне значення отриманих результатів полягає у можливості застосування

запропонованого підходу в системах, де одночасно існують неоднорідні інформаційні джерела, обмежені ресурси обробки та необхідність оперативного реагування на зміну ризикового стану. Важливо, що запропонована архітектура не прив'язана до конкретної предметної області на рівні базових механізмів. Зміна модальних енкодерів і специфічних ознак дозволяє адаптувати її до іншого типу інформаційних потоків без принципової перебудови механізму ризик-орієнтованого керування. Водночас отримані результати слід інтерпретувати з урахуванням обмежень проведеного дослідження. Окремим завданням є оцінювання стабільності моделі при перенесенні між різними предметними областями та часовими періодами, оскільки саме зміна розподілу даних може істотно впливати на достовірність ризикових оцінок. Перспективним напрямом подальшого розвитку є поглиблення адаптивності запропонованого методу шляхом переходу від однорівневого зважування модальностей до багаторівневого механізму, який одночасно враховуватиме якість джерела, часову актуальність інформації, мережеву доступність та прогнозований вплив конкретного потоку на кінцеве рішення. Доцільним є поєднання запропонованої архітектури з федеративним навчанням, що дозволить адаптувати моделі на локальних вузлах без централізованого накопичення первинних даних. Подальше вдосконалення ресурсного контуру може бути пов'язане із застосуванням багатоагентного навчання з підкріпленням, коли окремі вузли мережі навчатимуться узгоджено розподіляти обчислювальні, енергетичні та комунікаційні ресурси залежно від локального й глобального рівня ризику. У сукупності ці напрями створюють основу для переходу від адаптивного аналізу мультимодальних даних до самокерованих децентралізованих інтелектуальних мереж, у яких інформаційна якість, ризик і доступність ресурсів розглядаються як взаємопов'язані компоненти єдиного підходу прийняття рішень.

Література

[1] Gao, J., Li, P., Chen, Z., Zhang, J. A Survey on Deep Learning for Multimodal Data Fusion. Neural Computation. 2020. Vol. 32, No. 5. P. 829–864. DOI: 10.1162/neco_a_01273.

[2] Zhao, F., Zhang, C., Geng, B. Deep Multimodal Data Fusion. ACM Computing Surveys. 2024. Vol. 56, No. 9. Article 216. DOI: 10.1145/3649447.

[3] Jiao, T., Guo, C., Feng, X., Chen, Y., Song, J. A Comprehensive Survey on Deep Learning Multi-Modal Fusion Methods, Technologies and Applications. Computers, Materials & Continua. 2024. Vol. 80, No. 1. P. 1–35. DOI: 10.32604/cmc.2024.053204.

[4] Li, J., Hong, D., Gao, D., et al. Deep learning in multimodal remote sensing data fusion. International Journal of Applied Earth Observation and Geoinformation. 2022. Vol. 112. Article 102926. DOI: 10.1016/j.jag.2022.102926.

[5] Peng, K., Yan, G. A survey on deep learning for financial risk prediction. Quantitative Finance and Economics. 2021. Vol. 5, No. 4. P. 716–737. DOI: 10.3934/QFE.2021032.

[6] Fritz-Morgenthal, S., Hein, B., Papenbrock, J. Financial Risk Management and Explainable, Trustworthy, Responsible AI. Frontiers in Artificial Intelligence. 2022. Vol. 5. Article 779799. DOI: 10.3389/frai.2022.779799.

[7] Ch, R.K., Meenadevi, K., Kumar, D.D., Nagaraj, R. Deep Learning in Credit Risk Assessment: A Data-Driven Approach to Transforming Financial Decision-Making and

Risk Analytics. Journal of Risk and Financial Management. 2026. Vol. 19, No. 5. Article 361. DOI: 10.3390/jrfm19050361.
[8] Albeshri, M.Y., et al. Enhanced predictive modeling for financial risk assessment using hybrid AI (ML & DL) on structured and unstructured data. Discover Artificial Intelligence. 2026. DOI: 10.1007/s44163-026-01326-9.
[9] Cui, T., Yang, R., Fang, C., Yu, S. Deep Reinforcement Learning-Based Resource Allocation for Content Distribution in IoT-Edge-Cloud Computing Environments. Symmetry. 2023. Vol. 15, No. 1. Article 217. DOI: 10.3390/sym15010217.
[10] Aghapour, Z., Sharifian, S., Taheri, H. Task offloading and resource allocation algorithm based on deep reinforcement learning for distributed AI execution tasks in IoT edge computing environments. Computer Networks. 2023. Vol. 223. Article 109577. DOI: 10.1016/j.comnet.2023.109577.
[11] Zhao, J., Ni, Y., Cheng, Y. Joint Client and Resource Optimization for Federated Learning in Wireless IoT Networks. Applied Sciences. 2024. Vol. 14, No. 2. Article 542. DOI: 10.3390/app14020542.
[12] Cui, X., et al. Resource Allocation in IoT Edge Computing Networks Based on Reinforcement Learning. Intelligent Transportation and Smart Cities. 2026. DOI: 10.3233/ATDE250295.
[13] Aghapour, Z., Sharifian, S., Taheri, H. Task offloading and resource allocation algorithm based on deep reinforcement learning for distributed AI execution tasks in IoT edge computing environments. Computer Networks. 2023. Vol. 223. Article 109577. DOI: 10.1016/j.comnet.2023.109577.
[14] Qin, J., Yang, Y. Intelligent Green Resource Management for Blockchain-Powered IoT Networks Through Deep Reinforcement Learning. Internet Technology Letters. 2026. Vol. 9, No. 2. Article e70232. DOI: 10.1002/itl2.70232.
[15] Wadhwa, G., Natarajan, Y., Sri Preethaa, K.R., et al. Federated learning for sustainable IoT appliance load monitoring at the edge devices. Discover Sustainability. 2025. Vol. 6. Article 654. DOI: 10.1007/s43621-025-01409-0.
[16] Gao, J., Li, P., Chen, Z., Zhang, J. A Survey on Deep Learning for Multimodal Data Fusion. Neural Computation. 2020.Vol.32,No.5.P.829–864. DOI: 10.1162/neco_a_01273.
[17] Zhao, F., Zhang, C., Geng, B. Deep Multimodal Data Fusion. ACM Computing Surveys. 2024. Vol. 56, No. 9. Article 216. P. 1–36. DOI: 10.1145/3649447.
[18] Zhang, Q., Wei, Y., Han, Z., et al. Multimodal fusion on low-quality data. A comprehensive survey. Information Fusion. 2026. Vol. 135. Article 104437. DOI: 10.1016/j.inffus.2026.104437.
[19] Xu, P., Zhu, X., Clifton, D.A. Multimodal Learning With Transformers. A Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023. Vol. 45, No. 10. P. 12113–12132. DOI: 10.1109/TPAMI.2023.3275156.
[20] Zhou, J., Cui, G., Hu, S., et al. Graph neural networks. A review of methods and applications. AI Open. 2021. Vol. 1. P. 57–81. DOI: 10.1016/j.aiopen.2021.01.001.
[21] Waikhom, L., Patgiri, R. A survey of graph neural networks in various learning paradigms. Methods, applications, and challenges. Artificial Intelligence Review. 2023. Vol. 56. P. 6295–6364. DOI: 10.1007/s10462-022-10321-2.
[22] Chen, W., Hussain, W., Cauteruccio, F., Zhang, X. Deep Learning for Financial Time Series Prediction. A State-of-the-Art Review of Standalone and Hybrid Models. Computer Modeling in Engineering & Sciences. 2024. Vol. 139, No. 1. P. 187–224. DOI: 10.32604/cmes.2023.031388.
[23]Černevičienė, J., Kabašinskas, A. Explainable artificial intelligence in finance. A systematic literature review. Artificial Intelligence Review. 2024. Vol. 57. Article 216. DOI: 10.1007/s10462-024-10854-8.
[24]McMahan, H.B., Moore, E., Ramage, D., Hampson, S., Agüera y Arcas, B. Communication-Efficient Learning of Deep Networks from Decentralized Data. Proceedings of the 20th

International Conference on Artificial Intelligence and Statistics. 2017. Vol. 54. P. 1273–1282. DOI: 10.48550/arXiv.1602.05629.

[25]Chen, M., Wang, T., Zhang, S., Liu, A. Deep reinforcement learning for computation offloading in mobile edge computing environment. Computer Communications. 2021. Vol. 175. P. 1–12. DOI: 10.1016/j.comcom.2021.04.028.

[26]IEEE Computational Intelligence Society. IEEE-CIS Fraud Detection [Dataset]. Kaggle, 2019. https://www.kaggle.com/c/ieee-fraud-detection/data

[27]Chen, D. Online Retail [Dataset]. UCI Machine Learning Repository, 2015. DOI: 10.24432/C5BW33.

[28]Yeh, I.-C. Default of Credit Card Clients [Dataset]. UCI Machine Learning Repository, 2009. DOI: 10.24432/C55S3H.

[29]М. Д. Рудніченко, Д. В. Шведов, Н. О. Шибаєва, Т. В. Кунуп, І. М. Петров Гібридна модель аналізу мультимодальних даних на базі інтелектуальних агентів для оцінки інвестиційних ризиків у високоволатильні активи. Інформатика та математичні методи в моделюванні. 2026. №2. Т.16. С. 400-413. DOI 10.15276/imms.v16.no2.400

INTELLIGENT RISK-ORIENTED MULTIMODAL DATA ANALYSIS FOR ADAPTIVE RESOURCE CONTROL IN DECENTRALIZED NETWORKS

Ph.D., Rudnichenko M.[1], Ph.D., Shibaeva N.[1], Shumeiko K.[1], Shvedov D.[1], Zlenskiy A.[1], Dr.Sci.,Petrov I.[2]

[1]Odessa Polytechnic National University, Ukraine,

[2]National University "Odessa Maritime Academy", Ukraine

This paper presents a studyon the development of an intelligent risk-informed multimodal multidimensional data analysis method for adaptive resource management in decentralized networks, utilizing deep learning and adaptive information fusion mechanisms. The relevance of the study is driven by the growing volume of heterogeneous data in distributed digital environments, which demands the simultaneous assurance of risk analysis validity, processing speed, and the rational utilization of limited computational, communication, and energy resources.The limitations of traditional multimodal fusion strategies are analyzed, justifying the adoption of an adaptive architecture that accounts for the real-time quality of information modalities and risk levels when formulating control decisions. The proposed method integrates modality-specific data encoding, adaptive weighting of information streams, integrated latent representation formation, risk state estimation, and a closed-loop resource management framework for decentralized networks.An experimental testbed was implemented using Python, Jupyter Notebook, NumPy, Pandas, Scikit-learn, PyTorch, and Matplotlib. To construct an experimental data environment, open real-world datasets—specifically IEEE-CIS Fraud Detection, Online Retail, and Default of Credit Card Clients—containing transactional, temporal, behavioral, customer, and identification features were utilized. The proposed method was evaluated against early, late, and static weighted fusion approaches in terms of F1-score, ROC-AUC, processing latency, and energy consumption. Furthermore, the robustness of these methods under increasing resource workloads was assessed alongside an ablation study of the core architectural components. The experimental results demonstrate the superiority of the proposed approach in balancing risk analysis quality, adaptivity, and resource efficiency, confirming its promise for deployment in decentralized intelligent networks.

Keywords: *multimodal data fusion, data mining, risk-informed analysis, adaptive resource management, decentralized networks, deep learning, hybrid modelling, latent representation*

УДК 004.8:004. 932:632.4
DOI

ІНТЕЛЕКТУАЛЬНА СИСТЕМА ІДЕНТИФІКАЦІЇ ЗАХВОРЮВАНЬ РОСЛИН ЗА ЗОБРАЖЕННЯМИ НА ОСНОВІ ГЛИБОКОГО НАВЧАННЯ

Dr.Sci., Антощук С.[1][0000-0002-9346-145X],
Ph.D., Кунуп Т.[2][0000-0003-0246-0951], Кравченко О.[3][0009-0006-6982-0965]
Національний університет «Одеська Політехніка», Україна
EMAIL: [1]asg@op.edu.ua, [2]kunup.t.v@op.edu.ua,
[3]10253024@stud.op.edu.ua

Анотація. *У статті представлено всебічне дослідження щодо розробки системи ідентифікації захворювань рослин за допомогою алгоритмів машинного навчання. Мета роботи полягає в автоматизації процесу ідентифікації захворювань рослин по їхньому зовнішньому вигляду. Головним завданням роботи є розробка інтелектуального програмного забезпечення, здатного проводити швидкий і точний аналіз стану рослини по її фотографії. Визначено та реалізовано усі аспекти розробки системи визначення захворювань рослин по зображеннях. Проаналізовано існуючіпрограмні продукти, що використовуються для ідентифікації стану рослин, виявлено їхні переваги та недоліки, детально сформовано вимоги до функціоналу та якісних характеристик системи. Особливу увагу приділено згортковим нейронним мережам, їхнім принципам обробки зображень та видобування ознак, а також різним архітектурам. Проведено навчання декількох моделей різних мереж на наборах даних PlantVillage та PlantWild з метою порівняння їхньої точності. У розробленій системі застосовано модель, яка продемонструвала найбільший відсоток правильних передбачень на тестовому наборі даних, в якості якого було використано датасет PlantDoc. Програмний застосунок ідентифікації захворювань рослин реалізовано у вигляді мобільного додатку. Актуальність дослідження обґрунтована в тому, що усі часи існування сільського господарства людство стикалося з багатьма викликами для успішного збереження врожаїв. Однією з найбільших проблем є захворювання рослин, спричинені різними небезпечними чинниками. Станом на сьогодні, сучасні технології допомагають спростити та покращити діяльність людей у багатьох сферах, і сільське господарство не є винятком. Система, розроблена в рамках цього дослідження, стане легким у застосуванні інструментом для швидкого виявлення стану рослин, що допоможе працівникам фермерських господарств ефективніше вживати необхідних заходів для порятунку врожаю.*

Ключові слова: *класифікація зображень, ідентифікація захворювань рослин, згорткові нейронні мережі, глибоке навчання, PlantVillage, PlantWild, PlantDoc, штучний інтелект.*

Вступ

Сільське господарство – це одна з найважливіших сфер людської діяльності. Кількість людей, що працюють в аграрному секторі, становить приблизно 1 мільярд осіб, які складають 28% робочої сили всього світу. Такі дані не є дивними, адже рослинні продукти харчування є джерелом великої кількості поживних речовин, серед яких – вітаміни, мінерали, вуглеводи, жири та навіть білки. Рослинна їжа є не менш важливою за продукти тваринного походження, саме тому метою працівників фермерських господарств в усі часи є

забезпечення максимально високого рівня врожайності. Досягти успіху в цій справі – нелегка задача, адже на стан рослин впливають багато небезпечних чинників, наприклад: кліматичні проблеми, такі, як засуха та надмірна спека, повені, а також морози та гради; проблеми зі станом родючості ґрунтів, серед яких надмірне використання хімічних добрив та пестицидів, ерозії та засолення; залежність від інноваційних технологій, використання яких потребує додаткових знань і навичок та несе ризики щодо їхньої надійності; захворювання рослин, збудниками яких є бактерії, грибки, віруси, шкідники та паразитичні рослини [1, 2, 3]. Ризики, перераховані вище, можуть призвести до втрати вагомої частини виробленої продукції, що негативним чином відобразиться на отриманих доходах виробництва. Працівники аграрного сектору роблять усе можливе для того, щоби запобігти появі негативних наслідків або максимально зменшити їхній вплив, здійснюючи контроль поливів, використання добрив та засобів боротьби проти шкідників та хвороб. Проблема захворювань рослин є дуже серйозним викликом для сфери сільського господарства, тож рання діагностика та вчасне лікування є дуже важливими заходами. Сучасні науковці та агрономи постійно досліджують шляхи вдосконалення заходів боротьби проти поширення хвороб та мінімізації негативних наслідків. У роботі зроблено фокус на розробку програмного продукту, який дозволятиме швидко та точно виявити стан рослини та надати рекомендації щодо лікування постраждалих рослин. Проблема захворювань рослин є значно більш небезпечною, ніж може здаватися на перший погляд. За інформацією Продовольчої та сільськогосподарської організації ООН (Food and Agriculture Organization, FAO) хвороби рослин призводять до втрат приблизно у 40% урожаїв кожного року, що в свою чергу веде до величезних щорічних збитків, які оцінюються у 220 мільярдів доларів США. Трапляються й такі ситуації, коли ця проблема стає причиною ледь не повного знищення врожаю – наприклад, у деяких регіонах Кенії в 2013 – 2014рр. через хворобу летального некрозу було втрачено понад 90% урожаїв кукурудзи. Такі дані свідчать про те, що проблему захворювань сільськогосподарських культур неможливо ігнорувати, і велику важливість мають заходи вчасного діагностування та лікування рослин [4, 5]. Основними збудниками хвороб рослин є грибки, бактерії та віруси. Для вдалого розповсюдження ці мікроорганізми потребують спеціальних кліматичних умов, серед яких – рівень вологості, температури, освітлення, якості ґрунту тощо. Ще одним небезпечним фактором є діяльність комах-шкідників та паразитичних рослин.

З розвитком аграрних наук людство збагачувало свої знання про різні захворювання рослин – про їхні візуальні симптоми, збудників, швидкість розповсюдження, методи лікування та профілактики. Візуальні симптоми, авжеж, відіграють найважливішу роль у діагностуванні хвороби – для ідентифікації стану рослини необхідно перевірити її листя, плоди та стебло на наявність пошкоджень, плям і гнилі. Проведення зовнішнього аналізу рослин особисто агрономом є неефективним рішенням, адже такий підхід сильно залежить від кваліфікації фахівця, що проводить огляд, та може потребувати великої кількості часу. Однією зі складностей є також і візуальна схожість симптомів різних захворювань на початкових етапах розвитку хвороби. Ще

одним високоточним підходом є лабораторні дослідження уражених рослин з метою отримання детальної інформації про її стан. Цей метод, у свою чергу, є дорогим та недоступним для малих та віддалених фермерських господарств. Отже, виникає потреба у наявності легкодоступного інструменту, який проводитиме діагностику швидко і точно та не потребуватиме великої кількості ресурсів для своєї роботи. На допомогу приходять сучасні методи та технології зі сфер штучного інтелекту, машинного навчання та розробки програмного забезпечення, які вже активно використовуються для подолання існуючих проблем у напрямку теми роботи.

Аналіз наукових і технічних джерел, присвячених розпізнаванню зображень для ідентифікації та класифікації рослин, дає змогу визначити основні теоретичні положення, концепції та технологічні підходи, що формують сучасний стан досліджень у цій галузі. Результати попередніх досліджень створюють підґрунтя для розроблення високоефективних автоматизованих систем, призначених для використання в агрономії, екологічному моніторингу та освітніх застосуваннях. Одним із ключових напрямів сучасних досліджень є застосування методів глибокого навчання, зокрема згорткових нейронних мереж (Convolutional Neural Networks, CNN), які демонструють високу ефективність під час аналізу та класифікації візуальної інформації. Серед поширених архітектур, що використовуються для розпізнавання рослин, можна виділити AlexNet, VGGNet і ResNet. Зокрема, архітектура ResNet, використовує резидуальні зв'язки, що дає змогу зменшити негативний вплив проблеми згасання градієнта під час навчання глибоких нейронних мереж. Завдяки цьому забезпечується висока точність і стабільність класифікації рослин, зокрема за умов значної варіативності форми, структури та зовнішнього вигляду листя [6]. Важливим доповненням до методів класифікації є технології сегментації зображень, які забезпечують виділення цільового об'єкта з навколишнього середовища. У дослідженнях, присвячених застосуванню Mask R-CNN (He et al., 2017), сегментація використовується для точного відокремлення рослин від фону. Такий підхід є особливо актуальним для зображень, отриманих у природних або польових умовах, де на якість розпізнавання можуть впливати ґрунт, інші рослини, тіні та нерівномірне освітлення. Водночас застосування Mask R-CNN характеризується підвищеними вимогами до обчислювальних ресурсів, що може обмежувати його використання в системах із жорсткими вимогами до швидкодії [6]. Окреме місце в розвитку систем автоматизованого розпізнавання рослин посідають великі спеціалізовані набори даних. Дослідження проєкту PlantNet (Joly et al., 2016) демонструє ефективність краудсорсингового підходу до формування баз зображень. Залучення користувачів до збору та завантаження фотографій дає змогу створювати масштабні й різноманітні набори даних, що сприяє підвищенню здатності моделей розпізнавати широкий спектр видів, зокрема рідкісних. Водночас такий підхід створює додаткові проблеми, пов'язані з контролем якості, коректністю маркування та можливими помилками під час ідентифікації рослин користувачами. Важливу роль у підвищенні стійкості моделей до різноманітних умов отримання зображень відіграють методи аугментації даних. До найбільш поширених операцій належать обертання,

масштабування, зміна яскравості, контрастності та інших характеристик зображення. Застосування аугментації дає змогу розширити варіативність навчальної вибірки без необхідності пропорційного збільшення обсягів первинного збору даних. У результаті покращується узагальнювальна здатність моделі та її стійкість до змін умов зйомки [7]. Таким чином, аналіз наукових джерел свідчить, що поєднання методів глибокого навчання, сегментації та аугментації даних створює ефективну основу для розроблення систем автоматизованого розпізнавання рослин. Водночас актуальними залишаються питання забезпечення високої продуктивності таких систем на мобільних і периферійних пристроях, а також підвищення точності розпізнавання видів, для яких у доступних наборах даних представлена обмежена кількість зображень. Отже, сучасні методи забезпечують надійну технологічну основу для подальших досліджень, однак потребують адаптації до конкретних умов експлуатації та вимог кінцевих користувачів.

Актуальність автоматизованого розпізнавання рослин додатково зумовлена сучасними тенденціями розвитку аграрного сектору. Зростання чисельності населення планети, підвищення попиту на продовольство та інтенсифікація сільськогосподарського виробництва формують потребу в ефективнішому управлінні посівними площами. Водночас нестабільність кліматичних умов, поширення хвороб і шкідників можуть спричиняти значні економічні втрати та створювати ризики для продовольчої безпеки. За таких умов своєчасне виявлення патологічних змін у стані рослин, точна ідентифікація їхніх видів і визначення стадій розвитку набувають особливого значення для сучасного агромоніторингу та планування сільськогосподарського виробництва [8]. Традиційні методи польового моніторингу, що ґрунтуються переважно на візуальній оцінці стану рослин агрономами та використанні стаціонарних датчиків, не завжди забезпечують необхідну оперативність і масштабованість. Суб’єктивність людської оцінки, значні часові витрати та обмежена можливість одночасного контролю великих територій можуть призводити до затримки у виявленні проблем і прийнятті відповідних управлінських рішень. Додатковими обмеженнями є висока вартість частини спеціалізованого обладнання та необхідність оптимального використання трудових і матеріальних ресурсів. Це зумовлює потребу в технологіях, здатних поєднати точність, швидкість, масштабованість та економічну ефективність моніторингу.

Одним із перспективних технологічних рішень стало використання безпілотних літальних апаратів (БПЛА), оснащених високороздільними та багатоспектральними камерами. Застосування БПЛА дає змогу оперативно отримувати значні обсяги візуальної інформації про стан посівів із різних висот і ракурсів. Це розширює просторове охоплення моніторингу та водночас зменшує часові й трудові витрати. Використання багатоспектральних камер додатково забезпечує можливість аналізувати спектральні характеристики рослин, зокрема виявляти зміни, пов’язані зі станом листя та фотосинтетичною активністю. Такі ознаки можуть бути корисними для раннього виявлення стресових станів і потенційних уражень рослин.

Зростання обсягів візуальних даних, отриманих у результаті польового моніторингу, формує потребу в автоматизованих алгоритмах об'єктного детектування, здатних обробляти великі масиви зображень і відеокадрів із необхідною швидкістю та точністю. У цьому контексті особливий інтерес становлять моделі сімейства YOLO (You Only Look Once), орієнтовані на швидке виявлення об'єктів у зображеннях і відеопотоках. Сучасні версії, зокрема YOLOv8 та YOLO11, поєднують високу швидкість обробки з конкурентоспроможною точністю детектування, що робить їх перспективними для використання в системах автоматизованого агромоніторингу. Інтеграція моделей об'єктного детектування з даними, отриманими за допомогою БПЛА, відкриває можливості для автоматизованого виявлення та класифікації рослин, моніторингу їхнього стану, визначення ознак ураження та формування даних для подальшого прийняття управлінських рішень. Застосування таких технологій може сприяти підвищенню оперативності моніторингу посівів, раціональнішому використанню ресурсів і зменшенню потенційних втрат, пов'язаних із поширенням хвороб та шкідників [9].

1. Постановка проблеми та аналіз існуючих підходів та публікацій

Основною задачею системи є класифікація хвороб рослин по фотографіях листів чи плодів. Класифікація – це процес визначення категорії, до якої належить об'єкт в залежності від його ознак (характеристик). Першим етапом розробки системи стане навчання інтелектуальної моделі аналізувати зображення рослини та визначати, до якого класу вона належить – наприклад, «Яблуко здорове» або «Виноград, заражений хибною борошнистою росою» тощо. Перед безпосередньою реалізацією цього етапу необхідно провести ознайомлення з підходами, що можуть використовуватися в основі побудови такої класифікаційної моделі. Ці підходи базуються на архітектурі багатошарового перцептрона (Multilayer Perceptron, MLP). Це тип штучної нейронної мережі, який складається з декількох шарів – вхідного, одного чи двох прихованих та вихідного. Багатошаровий перцептрон є повнозв'язним (densely connected) – це означає, що всі нейрони попереднього шару мають зв'язки з усіма нейронами. MLP працює наступним чином:

- вхідний шар отримує початкові дані (наприклад, значення пікселів зображення чи слова тексту);
- кожен вхідний сигнал множиться на певне значення ваги та в прихованих шарах кожен нейрон обчислює зважену суму вхідних сигналів з додаванням зсуву (bias);
- застосовується нелінійна функція активації, яка дозволяє формувати складні залежності;
- результати обробки подаються на вихідний шар (у задач багатокласової класифікації кількість нейронів вихідного шару дорівнює кількості класів, кожне вихідне значення дорівнює значенню ймовірності приналежності елемента до відповідного класу).

Незважаючи на простоту архітектури та універсальність, завдяки якій багатошаровий перцептрон став основою для складніших підходів, він має такі недоліки, як низька швидкість та витрата великої кількості ресурсів для обробки великих наборів даних [13]. Рекурентні нейронні мережі (Recurrent

Neural Networks, RNN) – тип штучних нейронних мереж, призначений для опрацювання послідовних даних. Від традиційних прямопрохідних мереж їх відрізняє здатність зберігати інформацію попередніх кроків – на кожному кроці мережа враховує не тільки поточний вхід, а й результати обробки попередніх елементів послідовності даних (прихований стан). На кожному етапі обробки вхідного сигналу RNN обчислює новий прихований стан з використанням ваг та нелінійної функції активації. Після цього, обчислений новий прихований стан використовується як вхід на наступному кроці. У задачі ідентифікації хвороб рослин рекурентні нейронні мережі можуть бути використаними для спостереження за станом рослини у часі та розпізнавання різних стадій розвитку хвороби – від початкової до найбільш небезпечної. Але найкращим чином задачу аналізу зображень виконують інші підходи. Основним інструментом машинного навчання для аналізу зображень є згорткові нейронні мережі (CNN), про які вже було згадано раніше. Вони спеціально були спроєктовані саме для вирішення цієї задачі. Для обробки зображень згорткові нейромережі використовують алгоритм згортки, який полягає у застосуванні невеликого фільтра (ядра), наприклад, розміром 5×5 пікселів, який послідовно проходить по зображенню, обчислюючи скалярний добуток між вагами фільтру та значеннями пікселів, до яких було застосовано цей фільтр. Це допомагає визначати такі деталі фотографії, як межі, текстури та форми зображених об’єктів. Шари CNN, в яких використовуються операції згортки, називають згортковими шарами. Після згорткового шару зазвичай використовується шар активації, в якому застосовуються нелінійні активаційні функції, серед яких ReLU або Tanh. Для зменшення розмірності застосовуються шари об’єднання (pooling layers), вони бувають двох видів:

- Max pooling – з певної ділянки пікселів залишається лише той піксель, який містить найбільше значення;
- Average pooling – проводиться підрахунок середнього арифметичного значення пікселів певної ділянки.

Шари pooling зазвичай використовуються між шарами згортки. Вони допомагають збільшити швидкість обчислень, зменшити обсяги використання пам’яті та запобігти такому явищу, як перенавчання моделі – коли модель просто запам’ятовує дані, на яких навчається, але має труднощі з аналізом даних, які під час навчання не використовувалися.

Серед інших важливих елементів згорткової нейронної мережі:

- шар випрямляння, перетворює багатовимірні мапи ознак на одновимірний вектор для спрощення даних;
- повнозв’язний шар, виконує остаточну класифікацію;
- вихідний шар, визначає значення ймовірності приналежності елемента до кожного класу (від 0 до 1) застосовуючи функцію sigmoid для задач бінарної класифікації і softmax – для багатокласової [16].

Така структура робить CNN одним з найкращих алгоритмів для візуального аналізу зображень, дозволяючи швидко та точно виявляти важливі ознаки та проводити класифікацію. Станом на сьогодні існують можливості оптимізувати архітектуру мережі для роботи на малих пристроях, таких, як мобільні телефони, мікроконтролери та дрони. Усі перераховані вище складові елементи

CNN роблять їх придатними для створення високоточної системи визначення хвороб сільськогосподарських культур. Ще одним новим цікавим підходом для обробки зображень є трансформери бачення (Vision Transformers, ViT). Ця технологія була представлена у 2019 році. Вона була розроблена на основі трансформерів, що застосовувалися для аналізу тексту. У таких трансформерах елементи тексту перетворюються на токени, які потім конвертуються у вектори. За допомогою механізму multi-head attention сигнал ключових токенів посилюється, а для менш важливих – знижується. Візуальні трансформери працюють схожим чином – двовимірне зображення розбивається на патчі, з яких формуються одновимірний вектор. Мережа знає порядок та позицію кожного патчу у векторі. Наступний крок – додавання до послідовності патчів токена класифікації (CLS). Він здатний навчатися та використовується для збору глобальних ознак фотографії з усіх патчів. Його остаточний вихід використовується для класифікації без застосування операції pooling. Крім цього архітектура ViT використовує: механізм multi-head self-attention, який дозволяє аналізувати глобальні зв'язки між віддаленими частинами зображення, що дозволяє одночасно аналізувати різні типи інформації, такі, як межі, кольори, форми та текстури об'єктів на картинці; мережу прямого поширення (Fead-Forward Network, FFN), яка вивчає складні ознаки та застосовує складну нелінійну функцію активації GELU; залишкові / пропущені зв'язки між шарами (Residual / Skip Connections) для того, щоби запобігти втраті точності; архітектуру багатошарового перцептрона (MLP), застосовану до токена CLS для створення ймовірностей класів із застосуванням функції softmax. Такі складові елементи роблять архітектуру візуальних трансформерів дуже потужним інструментом для класифікації зображень, який демонструє високий рівень точності. Проте, незважаючи на всі переваги, ViT також має і недоліки, серед яких – потреба великої кількості ресурсів та необхідність навчання на наборах даних дуже великого обсягу. Для запуску на мобільних системах в останні роки зростає популярність використання архітектур, які поєднують риси згорткових нейронних мереж і трансформерів.

Сьогодні у відкритому доступі існує велика кількість уже розроблених архітектур згорткових нейронних мереж. Науковці, дослідники та розробники продовжують працювати над новими високоточними рішеннями класифікації зображень, розвиваючи цю сферу. Під час виконання роботи було проведено аналіз та навчання деяких архітектур CNN, спеціально оптимізованих під роботу на пристроях з не дуже великими обчислювальними потужностями, що робить можливим їхнє застосування у мобільних системах. Однією з широко відомих груп моделей згорткових нейронних мереж є EfficientNet, розроблена та представлена інженерами компанії Google у 2019 році. Особливістю цих моделей є застосування методу compound scaling, який полягає у масштабуванні параметрів глибини (кількості шарів), ширини (кількості каналів у шарах) та роздільної здатності вхідних зображень шляхом множення їхніх значень на певні визначені коефіцієнти. Група EfficientNet має всього 8 моделей згорткових нейронних мереж – від EfficientNet-B0 до EfficientNet-B7. Ці моделі відрізняються вимогами до ресурсів та цільовими задачами використання. Модель EfficientNet-B0 є найбільш компактною і саме вона була взята за основу

для створення інших моделей, від EfficientNet-B1 до EfficientNet-B7. Ця модель має широке застосування у реальних задачах аналізу фото, тож для класифікації хвороб рослин її теж можна використати.

Серед ключових особливостей цієї моделі можна визначити наступні характеристики:

- використання модифікованих інвертованих залишкових блоків MBConv, запозичених з моделі MobileNetV2;
- висока точність класифікації при невеликій кількості параметрів, яка досягається за допомогою підходу compound scaling;
- ефективне використання обчислювальних ресурсів;
- підтримка глибоких мереж без значного збільшення складності;
- використання механізму squeeze-and-excitation для покращення виділення важливих ознак.

Модель EfficientNet-B0 використовує меншу кількість параметрів у порівнянні з іншими архітектурами CNN, що робить її менш вимогливою до обчислювальних ресурсів, але не призводить до втрат точності.

Наступним сімейством згорткових нейронних мереж від компанії Google є MobileNet, спеціально призначена для роботи на смартфонах та вбудованих системах. Особливістю моделей цієї групи є використання згорток, розділених по глибині (depthwise separable convolutions), які допомагають зменшити кількість обчислень. У другій версії моделі (MobileNetV2) було представлено інвертовані залишкові блоки, робота яких полягає у початковому опрацюванні меншої кількості каналів з подальшим розширенням їхньої кількості. Це сприяє зменшенню складності моделі та підвищенню ефективності. Третя версія моделі (MobileNetV3) також використовує механізм squeeze-and-excitation та функцію активації h-swish. Для запуску на мобільних пристроях найбільше підходить модель MobileNetV3-Small. Серед її переваг – мала кількість параметрів, низьке енергоспоживання, висока швидкість інференсу та навіть можливість роботи в реальному часі.

Компанія Microsoft теж пропонувала свої рішення в цій сфері, одним з яких є дуже популярна група моделей ResNet, створена у 2015 році. Вона характеризується використанням залишкових блоків (residual blocks), які містять пропуски підключень між шарами (skip connections). Це допомагає запобігти втраті точності моделі, яка містить велику кількість шарів. ResNet-18 є відносно компактною мережею, що складається з 18 шарів. Її сильні сторони – це проста архітектура, висока точність та швидкість навчання. Модель широко використовується як базова архітектура у задачах комп'ютерного зору та може ефективно застосовуватись для класифікації захворювань рослин. Серед інших цікавих рішень вирізняється YOLO (You Only Look Once) від компанії Ultralytics – сімейство моделей, що здатні проводити ідентифікацію об'єктів у реальному часі. Представлено у 2015 році. Моделі YOLO також широко використовуються в задачах, де важливою є локалізація об'єкта на зображенні. Восьма версія моделей (YOLOv8) містить архітектуру YOLOv8-nano (YOLOv8n-cls) – найменшу та найшвидшу модель, що підходить для розгортання у мобільних системах. Серед особливостей цієї моделі можна підкреслити такі:

- використання C2f-блоків, які визначають як високорівневі семантичні ознаки, так і низькорівневі просторові дані – це призводить до підвищення точності, особливо під час виявлення малих об'єктів;

- anchor-free механізм для виявлення об'єктів, який усуває необхідність використання опорних блоків, що застосовувалися у старіших версіях YOLO і допомагали прогнозувати розташування об'єктів, вимагаючи ретельного налаштування та знання розмірів об'єктів.

Механізм anchor-free спрощує процес навчання та покращує продуктивність виявлення на різних масштабах об'єктів. DenseNet – архітектура, що характеризується повнозв'язністю шарів – кожен шар нейронної мережі з'єднаний з усіма наступними шарами. Ця її особливість відображена в назві – слово «dense» з англійської мови перекладається як «щільний». Такий підхід забезпечує ефективне повторне використання ознак та запобігає втраті точності.

Однією з найпопулярніших моделей цієї групи є DenseNet-121 – модель, що містить 121 шар згортки, серед них – 1 шар згортки 7×7, 58 шарів згортки 3×3 і 61 шар згортки 1×1. Також модель містить 4 шари average pooling та 1 шар fully connected. DenseNet-121 демонструє високу точність у задачах класифікації зображень та добре підходить для ідентифікації захворювань рослин, де важливим є виділення дрібних візуальних особливостей. Не менш цікавою для ознайомлення є архітектура ConvNeXt, запропонована організацією Meta у 2022 році. Вона об'єднує звичайні операції згортки з елементами візуальних трансформерів. Архітектура містить декілька різновидів моделей, серед яких найкомпактнішою є ConvNeXt-Tiny. Вона складається з чотирьох блоків (ConNeXt Block), які використовують велику глибоку згортку розміром 7×7, нормалізацію сигналів та застосування до них двошарового перцептрона 1×1 з функцією активації GELU або SELU. Використовуються також залишкові підключення (residual connections). Завдяки своїм характеристикам ConvNeXt-Tiny демонструє високу якість класифікації навіть на зображеннях, що містять різний рівень освітлення та шуму.

Ще однією гібридною архітектурою, яка поєднує риси згорткових нейронних мереж та трансформерів бачення є MobileViT, створена компанією Apple для мобільних систем комп'ютерного зору. Вона використовує операцію згортки розміром 3×3, залишкові блоки MobileNetV2 (MV2) для зменшення розмірності та блоки MobileViT, які поєднують переваги згорток та трансформерів. Моделі MobileViT ефективно виділяють глобальні та локальні ознаки, маючи низьку кількість параметрів, а така модель, як MobileViT-XXS, є однією з найкомпактніших, при цьому характеризується високою швидкістю роботи, енергоефективністю та високою точністю передбачень. Такі риси роблять її перспективною для застосування на мобільних пристроях. Після проведення аналізу декількох популярних архітектур згорткових нейронних мереж стає очевидною наявність великої кількості різних підходів, які забезпечують високу точність, високу швидкість навчання та при цьому низький рівень витрат обчислювальних ресурсів. Це свідчить про актуальність та розвиток застосування глибокого машинного навчання у сфері комп'ютерного зору. На подальших етапах роботи буде здійснено навчання

обраних моделей на певних наборах даних з метою порівняння різних метрик точності. Щоб моделі нейронних мереж навчилися розпізнавати ознаки захворювань різних рослин, їх необхідно натренувати на великих наборах зображень (датасетах). Саме датасети визначають точність, узагальнювальну здатність та практичну ефективність моделей машинного навчання. У сфері комп'ютерного зору для аграрних задач особливу роль відіграють набори даних, що містять зображення листя, плодів або стебел рослин із ознаками різних захворювань.

Одним із найвідоміших наборів даних у сфері розпізнавання захворювань рослин є датасет PlantVillage, презентований у 2016 році науковцями Федерельної Школи Технологій м. Лозан (Швейцарія) та Пенсильванського Державного Університету (США). Він став фактичним стандартом для навчання та тестування моделей класифікації рослинних захворювань. Датасет містить 54305 знімків листя рослин, що належать до 38 класів захворювань та здорових рослин для 14 культур, серед яких – фрукти, овочі, ягоди, злакові тощо. Основною особливістю PlantVillage є те, що всі зображення було отримано у лабораторних умовах. Листя фотографувалося на однорідному фоні при контрольованому освітленні, що значно зменшує вплив зовнішніх факторів.

Усі зображення мають розмір 256×256 пікселів. Окрім звичайної, існує також і версія цього набору даних з чорно-білими зображеннями, але в цій роботі вона не використовується. Знімки не містять аугментації – її планується застосувати безпосередньо перед початком навчання моделей нейронних мереж. Розмітка даних виконана в стилі «Культура__Назва__хвороби», наприклад, «Cherry_Powdery_mildew».

Перевагами PlantVillage є велика кількість зображень, якісна розмітка, збалансованість класів і простота використання для навчання CNN.[14-16] Проте цей набір даних має і певні недоліки, такі, як відсутність складного природного фону, обмежена варіативність умов зйомки та слабка узагальнювальна здатність моделей у реальних польових умовах. Дослідження, проведене у 2024 році, показало, що модель, точність якої на датасеті PlantVillage становила 99.35%, при тестуванні у польових умовах змогла правильно класифікувати рослину та її хворобу лише в 40% випадків.

Ще одним недоліком цього набору даних є те, що кількість зображень не є ідеально збалансованою по класах – деякі класи мають значно більше знімків, наприклад, 43.4% зображень PlantVillage становлять фотографії томатів, що може призвести до упередженості моделі. Більш детальний аналіз кількості зображень наведено у таблиці 1.

Аналіз набору даних PlantVillage показав, що хоч він і є одним з найпопулярніших, має суттєві недоліки та його може бути недостатньо для ефективного навчання моделей. Подолати цю проблему можна використовуючи метод навчання, який має назву Transfer Learning. Підхід трансферного навчання (Transfer Learning) описується таким чином – модель, навчена для виконання одного завдання, проходить повторне навчання для вирішення пов'язаного завдання, яке може бути більш складним та конкретизованим. Це допомагає підвищити ефективність та швидкість

навчання, при цьому знизити рівень обчислювальних витрат. У задачі тренування моделей для ідентифікації хвороб рослин метод Transfer Learning можна застосувати наступним чином: здійснити попереднє навчання (pretrain) на датасеті PlantVillage, який складається з лабораторних зображень, а завершення навчання (fine-tune) реалізувати на складнішому наборі даних, який містить фотографії, зроблені у польових умовах. Отже, поставлена задача потребує використання набору зображень зі складнішим фоном та різними умовами освітлення. Такі вимоги задовольняє датасет PlantWild, який містить 89 класів для 33 різних культур.

Таблиця 1

Розподіл зображень надору даних PlantVillage по класах

Культура	**Кіл-ть класів**	**Кількість зображень на кожен клас**	**Загальна кіл-ть зображень**
Яблуко	4	Apple Scab – 630; Apple Black Rot – 621; Apple Cedar Rust – 275; Apple Healthy – 1645	3171
Чорниця	1	Blueberry Healthy – 1502	1502
Вишня	2	Cherry Powdery Mildew – 1052; Cherry Healthy – 854	1906
Кукурудза	4	Corn Cercospora Leaf Spot – 513; Corn Common Rust – 1192; Corn Northern Leaf Blight – 985; Corn Healthy – 1162	3852
Виноград	4	Grape Black Rot – 1180; Grape Esca – 1383; Grape Leaf Blight – 1076; Grape Healthy – 423	4062
Апельсин	1	Orange Haunglongbin – 5507	5507
Персик	2	Peach Bacterial Spot – 2297; Peach Healthy – 360	2657
Перець	2	Pepper Bell Bacterial Spot – 997; Pepper Bell Healthy – 1478	2475
Картопля	3	Potato Early Blight – 1000; Potato Late Blight – 1000; Potato Healthy – 152	2152
Малина	1	Raspberry Healthy – 371	371
Соєвий біб	1	Soybean Healthy – 5090	5090
Кабак	1	Squash Powdery Mildew – 1835	1835
Полуниця	2	Strawberry Leaf Scorch – 1109; Strawberry Healthy – 456	1565
Томат	10	Tomato Bacterial Spot – 2127; Tomato Early Blight – 1000; Tomato Late Blight – 1909; Tomato Leaf Mold – 952; omato Septoria Leaf Spot – 1771; Tomato Spider Mites – 1676; Tomato Target Spot – 1404 Tomato Mosaic Virus – 373; Tomato Yellow Leaf Curl Virus – 5257; Tomato Healthy – 1591	18060

Кількість фотографій – 18542, всі вони зроблені у полі при різних погодних. Об’єкти на знімках мають різні розміри, також трапляються часткові перекриття листя та шуми. Такі характеристики роблять PlantWild вдалим

вибором для навчання моделей для реальних аграрних умов. Особливістю PlantWild також є наявність файлу типу JSON, який містить текстові описи візуальних ознак кожного класу (по 50 описів на клас), що дозволяє проводити мультимодальне навчання та використовувати vision-language моделі. Набір даних вперше було представлено у 2024 році вченими з Університету Квінсленда (Австралія). Серед інших датасетів, вартих уваги, вирізняється PlantPAD – один з найбільших існуючих наборів знімків рослин. У його розробці бере участь університет м. Стенфорд, США. PlantPAD містить 421314 зображень для 310 захворювань 63 видів рослин, серед яких найбільш присутніми є томати, кукурудза, яблуко, виноград, картопля тощо. Дані було зібрано з інтернет-джерел, наукових публікацій та інших відкритих датасетів. Окрім візуальної інформації містить також і текстові описи симптомів. Назви класів виглядають як «культура_назва_хвороби», наприклад, «tomato_early_blight». Датасет містить як лабораторні, так і польові зображення, до яких застосовано такі методи аугментації, як легка зміна налаштувань кольору (яскравості, контрастності, насиченості), поворот на певний кут, дзеркальне відображення по вертикалі чи горизонталі. Знімки мають різну розмірність – це зумовлено тим, що вони були зібрані з різних джерел. Незважаючи на такі переваги, як велика кількість даних та різноманітність культур, набір даних має основний недолік – значна неоднорідність даних, причиною якої є витягнення зображень з великої кількості різних джерел. Це ускладнює навчання моделей та вимагає складнішої попередньої обробки. Цікавим датасетом є PlantSeg, особливість якого полягає у наявності масок сегментації, зроблених авторами вручну, які виділяють уражену область рослини на зображенні. Цей набір даних було створено дослідниками Університету Квінсленда (Австралія) та опубліковано на початку 2026 року. Усього він містить 11458 зображень, зібраних з відкритих джерел, для 115 захворювань і охоплює 34 культури. PlantSeg є погано збалансованим набором даних: найменший клас (peach rust) містить усього 8 знімків, а найбільший (citrus canker) – 390. Класи називаються так само, як і у PlantWild. Крім того, так само, як і PlantPAD, PlantSeg має знімки різних розмірів. Методи аугментації не застосовуються. Усі зображення зроблені в польових умовах, що дозволяє моделі навчитися виявляти важливі ознаки у складному оточенні, а високоточні сегментаційні маски, про які було зазначено раніше, дозволяють визначити межі ураження й оцінити ступінь пошкодження рослини. Датасет чудово підходить для навчання таких моделей, як YOLO та U-Net, які спеціалізуються на локалізації елементів зображення.

Ще одним набором даних, орієнтованим на реальні умови зйомки, є PlantDoc, створений науковцями з Індійського Технологічного Університету м. Гадінаґар. Він був представлений у 2020 році якраз як альтернатива для PlantVillage, який складається лише з лабораторних знімків. Датасет містить 2598 зображень, які відображають 27 класів захворювань для 13 видів рослин. Кожен клас містить від 54 до 191 зображення. Найменування класів здебільшого представлені у вигляді «Культура назва хвороби», наприклад, «Tomato leaf yellow virus», але в деяких класах назва захворювання теж починається з великої літери (до прикладу, «Apple Scab leaf»), а у класах

винограду назва культури написана з букви нижнього регістру («grape leaf black rot»). Тобто, якість розмітки даних не доведена до ідеалу. Методи аугментації не були застосовані до зображень. Як і у випадку з PlantPAD, зображення були зібрані з різних інтернет-джерел у відкритому доступі за допомогою пошукових браузерів Google та Ecosia. Через це його дані є неоднорідними, однак вони добре відображають реальні умови використання систем діагностики рослин, тож моделі, які навчаються на PlantDoc, мають високу точність та здатність до узагальнень. Основним недоліком є малий обсяг даних. Підсумовуючи, варто зазначити, що сучасні набори даних для ідентифікації захворювань рослин суттєво відрізняються за обсягом, типом анотацій та умовами отримання зображень. Лабораторні датасети, такі, як PlantVillage, забезпечують високу якість та простоту навчання моделей, тоді як польові набори даних PlantWild, PlantSeg та PlantDoc дозволяють створювати більш стійкі системи, здатні працювати у реальних умовах. Використання великих та різноманітних датасетів є одним із ключових факторів підвищення точності та надійності систем автоматичної діагностики захворювань рослин. Ідея створення програмних продуктів для визначення хвороб рослин не є новою – у відкритому доступі вже існують такі застосунки. У цьому розділі будуть проаналізовані різні існуючі рішення, їхні переваги та недоліки. Імовірно, найбільш розповсюдженою програмою для садівництва є Plantix. Німецька організація PEAT Gmbh розробила її у вигляді мобільного застосунку для операційної системи Android у 2015 році . З того моменту Plantix було завантажено більше 10 мільйонів разів з ресурсу Google Play. У процесі розробки були використані алгоритми глибокого навчання для забезпечення можливості аналізу стану рослини. Програма надає користувачу можливість сфотографувати рослину, після чого визначає її стан та надає рекомендації з догляду та лікування. Аналіз фотографії триває 1.7 секунди, система розпізнає більш ніж 780 захворювань для 82 видів культур. Крім цієї базової операції, Plantix містить велику кількість корисних функцій, серед яких: доступ до бібліотеки корисних матеріалів з порадами щодо вирощування різних видів рослин – користувач може обрати до 8 культур, які його цікавлять; отримання сповіщень про спалахи певних хвороб у регіоні користувача; обговорення різних питань зі сфери сільського господарства на форумі – у спільноті користувачів є досвідчені агрономи, які можуть надавати різні поради; калькулятор добрив, який надає можливість розрахувати необхідну кількість поживних речовин в залежності від розміру ділянки, на якій посаджено рослини; підбір найкращого моменту для проведення обприскування та фумігації (обробки рослин газоподібною речовиною для боротьби проти шкідників та захворювань) в залежності від погодних умов.

Ще однією відомою мобільною програмою для рослинництва є Agrio. Розроблена ізраїльською компанією Saillog Ltd у 2017 році, станом на сьогодні вона нараховує більш ніж 500 тисяч завантажень з Google Play. Як і Plantix, застосунок Agrio має наступний функціонал: ідентифікація захворювань рослин по фотографіях – всього 500 хвороб; швидкість визначення стану рослини є нижчою, ніж у Plantix; наявність бібліотеки з рекомендаціями щодо лікування та догляду за рослинами; сповіщення користувача про

розповсюдження захворювань та шкідників у його регіоні. Також існують програми, здатні ідентифікувати хвороби лише певних видів рослин, наприклад, мобільні застосунки Tumaini та Tumaini Bean для банану та квасолі відповідно. Серед масштабніших рішень можна виділити систему Watson Decision Platform for Agriculture, розроблену компанією IBM у 2019 році. Програма використовує алгоритми штучного інтелекту та технології Інтернету речей для надання точних прогнозів погоди та залежних від них рекомендацій по догляду за посівами. Також система здатна відстежувати стан полів за допомогою супутникового моніторингу і підказувати аграріям оптимальну кількість води та добрив на основі даних, отриманих від сенсорів, що аналізують стан ґрунтів. Досвід використання Watson Decision Platform в Індії показав, що ці корисні функції допомогли скоротити об'єм витрат води та пестицидів на 25% та 40% відповідно. Ба більше, ця платформа також допомагає піклуватися про врожаї вже після збору – рекомендує оптимальні умови зберігання та доставки, базуючись на значеннях температури, вологості та часу в дорозі. Після запуску системи у Кенії та Нігерії вдалося скоротити втрати продуктів харчування після збору врожаю на 18%.

Платформа Watson Decision надає широкий спектр корисного функціоналу, але через свої особливості є орієнтованою лише на великі фермерські господарства з достатнім рівнем цифровізації. Окрім систем для ідентифікації стану сільськогосподарських культур існують також і такі програми, як Picture This і Plantify, орієнтовані на кімнатні рослини [9]. На додачу до цих та інших програмних рішень, цікавими для ознайомлення є різноманітні моделі нейронних мереж, запропоновані науковцями для забезпечення високої точності у сфері визначення захворювань рослин. Наприклад, однією з таких моделей є ConViTX. Її архітектура є доволі компактною та використовує поєднання згорткових нейронних мереж та візуальних трансформаторів для одночасного виявлення локальних та глобальних ознак. Модель було протестовано на наборі даних, складеному авторами дослідження з польових зображень кукурудзи, і її точність досягла значення у 98.8% правильних передбачень, що робить її перспективним рішенням для застосування [10].

Ще одна модель, варта уваги – MSCVT. Її архітектура є подібною до ConViTX – вона поєднує переваги згорткових нейронних мереж та візуальних трансформаторів. Також модель використовує інвертований залишковий блок, який допомагає зменшити кількість параметрів, що робить модель менш вибагливою до обчислювальних ресурсів. Точність MSCVT склала 99.86% та 97.5% на двох різних наборах даних [11, 12, 13, 14, 15]. Серед проаналізованих програмних рішень можна виявити такі недоліки, як обмежена точність при роботі з зображеннями низької якості й обмежена доступність у віддалених районах (зокрема через потребу підключення до мережі Інтернет або складної архітектури системи). Втім, висока точність моделей нейронних мереж, які використовуються для визначення хвороби рослини по фото, робить цей напрямок перспективним та вартим подальших удосконалень.

2 Формалізація задачі та розроблення запропонованої системи

Для розробки системи ідентифікації захворювань рослин за допомогою алгоритмів машинного навчання було обрано ефективні програмні засоби, що

забезпечують можливість підготовки даних, навчання нейронних мереж, тестування моделей та їх подальшої оптимізації для використання на мобільних і вбудованих пристроях. У даній роботі для реалізації системи було обрано сучасний стек технологій, який включає мову програмування Python, хмарне середовище Google Colab та набір спеціалізованих бібліотек для глибокого навчання і комп'ютерного зору. У сфері штучного інтелекту, машинного навчання та аналізу даних Python є однією з найпопулярніших мов програмування – це обумовлено простим синтаксисом, великою кількістю бібліотек та активною спільнотою розробників. Також важливими перевагами є висока швидкість виконання коду та легка інтеграція з іншими технологіями C/C++, Java тощо. У сфері комп'ютерного зору та аналізу зображень мова Python фактично є стандартом завдяки наданню зручних засобів для попередньої обробки зображень, підготовки навчальних вибірок, навчання нейронних мереж та експорту моделей для подальшого використання на цільових пристроях. Навчання моделей нейронних мереж та оцінка їхньої точності проведена на платформі Google Colab. Вона базується на іншій подібній платформі – Jupyter Notebook, надає можливість запускати код, написаний мовою Python, без налаштування локального середовища і використовувати графічні (GPU) або тензорні процесори (TPU) для прискорення обчислень. Підтримується інтеграція з Google Drive та можливість спільної роботи над проєктами.

Однією з бібліотек, що будуть використані у процесі навчання моделей, є TensorFlow від компанії Google. За допомогою TensorFlow можна створювати нейронні мережі, визначаючи архітектуру, шари, функції активації, кількість епох навчання та інші параметри. Для створення мобільних систем штучного інтелекту особливо важливою є бібліотека TensorFlow Lite, яка оптимізує моделі для подальшого запуску на мобільних та вбудованих пристроях, зменшуючи розмір моделей і забезпечуючи підтримку ARM-процесорів. Такі моделі зберігаються у вигляді файлів з розширенням *.tflite і під час роботи характеризуються низьким енергоспоживанням та високою швидкістю виконання класифікації. Ще однією популярною бібліотекою, яку планується застосувати, є PyTorch, розроблена компанією Meta. Станом на сьогодні вона широко використовується у наукових дослідженнях та AI-розробці завдяки гнучкості та зручності роботи. Так само, як і TensorFlow, вона використовується для побудови нейронних мереж, а також підтримує трансферне навчання та ефективну роботу з великими обсягами даних. Однією з основних переваг PyTorch є підтримка dynamic computational graph – налаштування, яке дозволяє змінювати архітектуру мережі вже після початку навчання. Серед основних елементів PyTorch, які будуть використовуватися під час навчання моделей, можна виділити наступні: модуль torch.nn – для побудови архітектури мереж, який містить різні шари, функції активації та інші елементи, а також дозволяє реалізувати архітектури таких нейромереж, як ResNet; DenseNet, MobileNet, ConvNeXt і MobileViT; модуль torch.optim – для оптимізації параметрів моделі під час навчання з метою оновлення ваг та збільшення точності; модуль torch.utils.data – для роботи з наборами даних, зокрема для завантаження та розподілу на тренувальні та валідаційні вибірки.

Офіційною бібліотекою комп'ютерного зору для PyTorch є Torchvision. Вона містить готові датасети, інструменти аугментації, попередньо навчені моделі та функції обробки зображень. Серед складових елементів Torchvision, які планується використати: модуль transforms – для застосування до зображень методів аугментації, таких, як зміни розміру зображень, випадкові повороти, віддзеркалення, розмиття, зміна насиченості та контрастності тощо; модуль models містить CNN-архітектури: ResNet, DenseNet, MobileNet, ConvNeXt та EfficientNet. Бібліотека TorchAO надає можливість оптимізувати моделі, зменшивши їхні розміри за допомогою алгоритму квантизації, при цьому не завдавши суттєвих втрат для точності, а бібліотека ONNX2TF дозволяє здійснити конвертацію моделі у формати TensorFlow та TensorFlow Lite [16]. Отже, обраний набір програмних засобів забезпечує повний цикл роботи з моделями нейронних мереж - від підготовки даних та навчання нейронних мереж до оптимізації моделей і їх інтеграції у мобільну систему ідентифікації захворювань рослин. Фінальний і ключовий етап роботи – це, власне, сама розробка мобільної програми виявлення захворювань сільськогосподарських культур. Щоби відповідати усім поставленим вимогам, у розробці застосунку мають використовуватися найсучасніші програмні засоби та технології.

В якості мови програмування було обрано Kotlin, яка використовується для розробки більшості мобільних додатків для операційної системи Android. Ця мова розроблюється з 2010 року, її особливостями є повна сумісність з Java-бібліотеками, лаконічний синтаксис, статична типізація, можливість багатопотокової роботи і null-safety, тобто наявність окремих типів даних для значень, які можуть дорівнювати null (такі типи даних називаються nullable).

Розробка системи здійснювалася в інтегрованому робочому середовищі (Integrated development environment, IDE) Android Studio, яке підтримує такі мови для розробки Android-застосунків, як Kotlin, Java та C++. Android Studio надає інструменти для створення інтерфейсу, тестування застосунку, емуляції пристроїв з операційною системою Android та контролю версій, а також дозволяє вибір Android SDK. Для створення графічного інтерфейсу користувача (graphic user interface, GUI) було використано бібліотеку Jetpack Compose. Її особливість полягає у відсутності роботи з XML – елементи інтерфейсу визначаються засобами мови Kotlin, що спрощує роботу та зменшує кількість коду. Бібліотека підтримує створення адаптивних інтерфейсів, анімацій та можливість динамічного оновлення елементів інтерфейсу відповідно до стану застосунку. Для роботи з зображеннями, отриманими за допомогою камери чи галереї пристрою, використовується вбудована бібліотека Bitmap. Для запуску моделі типу tflite застосовується TensorFlow Lite Interpreter – бібліотека мови Java, яка дає можливість ефективно виконувати інференс моделей нейронних мереж із мінімальним споживанням ресурсів пристрою. В якості локального сховища даних про користувачів та їхні збережені рослини використовується база даних Room, яка є бібліотекою абстракції над SQLite і входить до набору Kotlin-бібліотек Jetpack. Room використовує об'єктно-орієнтований підхід для роботи з даними, а також підтримує перевірку SQL-запитів під час компіляції, інтеграцію з Kotlin Coroutines та архітектурними компонентами Android. Підсумовуючи

проведений аналіз засобів розробки та їхніх характеристик, можна зробити висновок, що підібраний стек розробки забезпечить усі можливості для створення легкого у використанні та швидкого в роботі програмного забезпечення.

2.1 Навчання моделей нейронних мереж та аналіз результатів

Навчання моделей відбувається у два етапи – pretrain на наборі даних PlantVillage, який складається з лабораторних зображень рослин, і fine-tune на датасеті PlantWild, що складається з фотографій рослин, зроблених у природніх умовах. Для pretrain відведено 30 епох тренування, для fine-tune – 60. Fine-tune розділено на фази A та B: у першій (15 епох) тренувалися лише останні шари класифікації (classification head), а у другій (45 епох) – вся модель (head + backbone). Під час виконання дослідження було проведено навчання таких моделей згорткових нейронних мереж, як EfficientNet-B0, MobileNetV3-Small, DenseNet-121 і ConvNeXt-Tiny. Модель EfficientNet-B0 показала такі результати точності: етап pretrain на PlantVillage – 99.97% на тестовій вибірці, 99.89% – на валідаційній; етап fine-tune на PlantWild – 38.90% на тестовій вибірці, 60.59% – на валідаційній; тестування на PlantDoc – 46.28% випадків надання правильній хворобі найбільшої ймовірності, 83,23% випадків потрапляння правильної хвороби у топ-5 наймовірніших.

Графіки, які відображають послідовний прогрес точності моделі EfficientNet-B0 з кожною епохою навчання, наведені на рис. 1 і рис. 2.

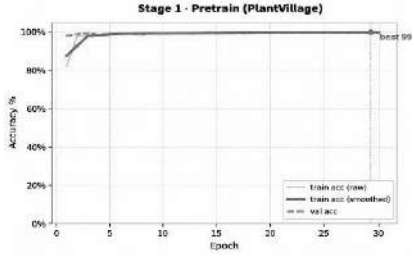


Рисунок 1. Навчання моделі EfficientNet-B0, етап pretrain

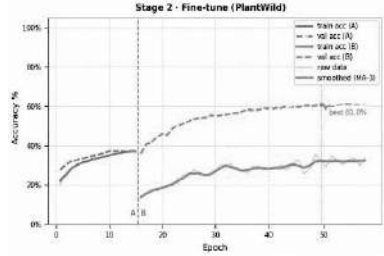


Рисунок 2. Навчання моделі EfficientNet-B0, етап fine-tune

Модель MobileNetV3-Small має гірші результати: етап pretrain на PlantVillage (рис. 3) – 99.97% на тестовій вибірці, 99.78% – на валідаційній; етап fine-tune на PlantWild (рис. 4) – 32.58% на тестовій вибірці, 51.45% – на валідаційній; - тестування на PlantDoc – 35.22% випадків надання правильній хворобі найбільшої ймовірності, 69.38% випадків потрапляння правильної хвороби у топ-5 найімовірніших.

Модель DenseNet-121 продемонструвала себе відносно непогано:

- етап pretrain на PlantVillage – 99.98% на тестовій вибірці, 99.88% – на валідаційній (рис. 5);

- етап fine-tune на PlantWild – 35.97% на тестовій вибірці, 58.62% – на валідаційній (рис. 6);

- тестування на PlantDoc – 48.38% випадків надання правильній хворобі найбільшої ймовірності, 82.47% випадків потрапляння правильної хвороби у топ-5 найімовірніших.

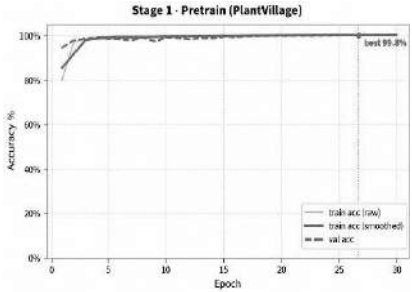


Рисунок 3. Навчання моделі MobileNetV3-Small, етап pretrain

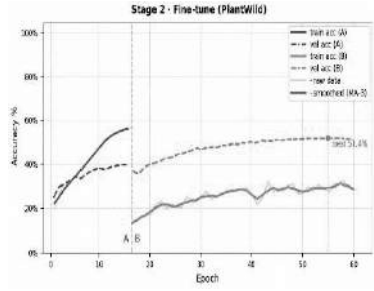


Рисунок 4. Навчання моделі MobileNetV3-Small, етап fine-tune

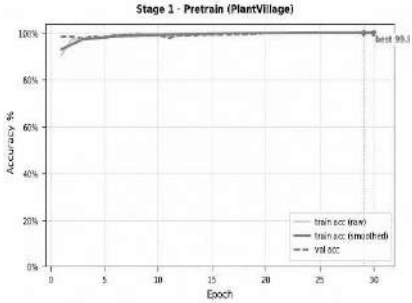


Рисунок 5. Навчання моделі DenseNet-121, етап pretrain

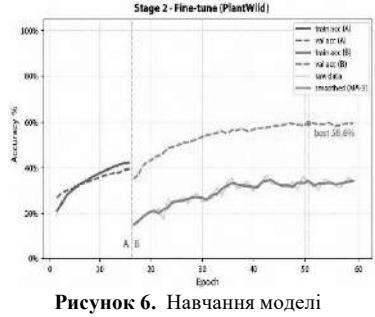


Рисунок 6. Навчання моделі DenseNet-121, етап fine-tune

Моделлю з найкращими результатами серед усіх є ConvNeXt-Tiny. Вона продемонструвала наступні показники точності: етап pretrain на PlantVillage – 98.12% на тестовій вибірці, 99.01% – на валідаційній (рис.7); етап fine-tune на PlantWild – 47.05% на тестовій вибірці, 72.17% – на валідаційній (рис..8); тестування на PlantDoc – 62.65% випадків надання правильній хворобі найбільшої ймовірності, 90.52% випадків потрапляння правильної хвороби у топ-5 найімовірніших.

Замість визначених 30 епох, навчання моделі на етапі pretrain тривало усього 9 епох через механізм EarlyStopping, який було застосовано, бо точність моделі не зростала з першої епохи. Модель ConvNeXt-Tiny має найвищі показники точності, тож у мобільному застосунку було прийнято рішення використовувати саме її. Навчання кожної моделі зайняло приблизно 30 хвилин. Для максимального пришвидшення цього процесу в Google Colab було використано графічний процесор G4, який має 95 ГБ оперативної пам'яті. Оглянувши результати навчання, можна зробити наступний висновок – усі моделі показали спроможність швидко навчитися точно вирізняти хвороби рослин на датасеті PlantVillage, усі фотографії якого були зроблені в однакових умовах з простим фоном, а при переході на набір даних PlantWild зі складнішими знімками рослин у природному оточенні задача правильно навчитися проводити класифікацію стала значно складнішою.

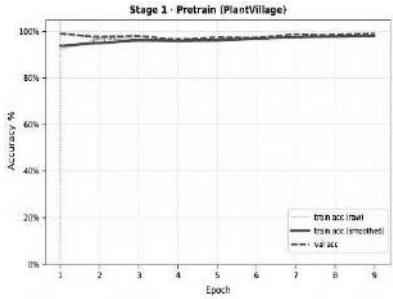


Рисунок 7. Навчання моделі ConvNeXt-Tiny, етап pretrain

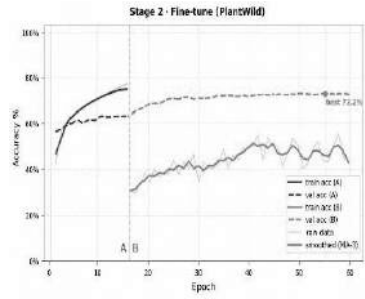


Рисунок 8. Навчання моделі ConvNeXt-Tiny, етап fine-tune

2.2 Проєктування мобільного застосунку ідентифікації стану рослин

Маючи сформовані функціональні та нефункціональні вимоги до мобільного застосунку, а також визначившись з набором засобів розробки, цілком влучним заходом стане планування проєкту додатку. Цей етап дозволить визначити усі аспекти поведінки системи, її взаємодію з користувачем і сценарії використання.



Рисунок 9. Діаграма використання

Під час проєктування мобільного застосунку було використано уніфіковану мову моделювання, яка допомагає здійснити опис архітектури системи, її складових елементів та основних процесів шляхом побудови діаграм. Візуалізація цих аспектів за допомогою UML допомагає краще зрозуміти усі деталі системи, яку планується розробити. Буває так, що UML-діаграми використовуються для опису логіки вже розробленого програмного забезпечення і становлять важливу частину його документації. У роботі було створено діаграму варіантів використання програми (Use case diagram) та діаграму послідовності (Sequence diagram) процесу діагностування рослини. Діаграма варіантів використання (також відома як діаграма прецедентів) призначена для демонстрації дій, які користувач може здійснювати у програмі. Якщо функціонал програми передбачає різні ролі користувачів, які мають різний рівень доступу до функціоналу програми, на діаграмі це має бути враховано. Use case діаграма для мобільного застосунку виявлення хвороб рослин наведена на рис. 9. На ній послідовно відображені усі дії, які програма надає користувачеві.

3 Дослідження роботи та обчислювальні експерименти

Експериментальні дослідження були спрямовані на оцінювання ефективності запропонованої системи та перевірку її здатності використання та отримання результатів. На початку робота в застосунку починається з реєстрації. Якщо користувач уже має обліковий запис у системі, то він може авторизуватися. Реєстрація та авторизація включають введення адреси електронної пошти та пароля. Пройшовши цей етап, користувач отримує доступ до використання функціоналу системи. Мобільна програма визначення захворювань сільськогосподарських культур проводить ідентифікацію стану рослини після її візуального огляду. Для його вдалого здійснення система потребує лише однієї фотографії ураженого листя чи плоду рослини, яку користувач може надати двома способами – скориставшись камерою мобільного телефону або його галереєю. Після проходження етапу отримання зображення система аналізує його та надає відповідь про його стан, яка включає вид рослини, її діагноз та короткі рекомендації з лікування. Отримані результати користувач може зберегти до бази даних.

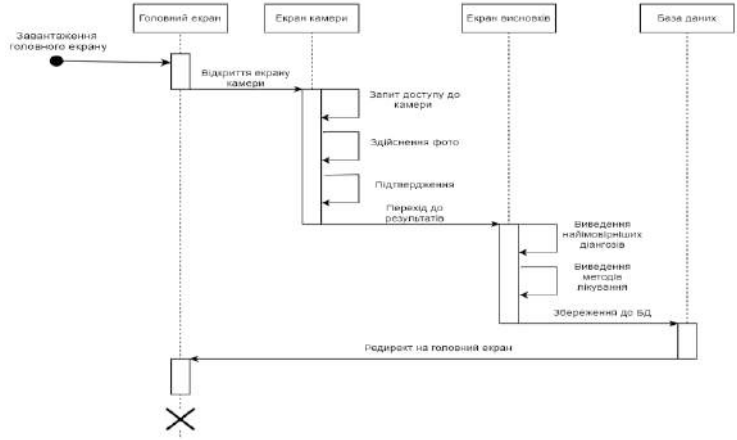


Рисунок 10. Діаграма послідовності діагностування зображення

Функціонал програми також включає можливість редагування даних профілю, а саме – зміну адреси електронної пошти, пароля й імені користувача. Крім цього, користувач також може видалити свій профіль разом з усіма даними, якщо більше не бажає працювати з програмою.

На рис.10 наведено діаграму послідовності діагностування рослини в застосунку. Ця діаграма відображає дії, які здійснюються різними компонентами системи під час проходження процесу отримання діагнозу рослини, а також переходи між компонентами.Екран результатів виводить перелік з 5 найімовірніших діагнозів та методів лікування для кожного з них. Цей екран надає користувачу можливість зберегти результати діагностики до бази даних. Збереження результатів дозволяє реалізувати функцію історії розпізнавань. Після успішного входу в систему користувач потрапляє на головну сторінку застосунку, яка містить короткий опис програми та кнопку

«Diagnose», яка перенаправляє користувача на сторінку вибору зображення. Можна скористатися камерою для здійснення фотографії ураженої рослини, а також обрати необхідний знімок з галереї смартфону. Наступний етап – проведення моделлю нейронної мережі аналізу зображення з метою виявлення рослини, яка відображена на ньому, та її захворювання. У програму інтегровано модель convnext_tiny_fp32_litert.tflite, яка мала найвищі показники точності за підсумками навчання.



Рисунок 11. Графічний інтерфейс сторінки результатів діагностики

Наступний етап – проведення моделлю нейронної мережі аналізу зображення з метою виявлення рослини, яка відображена на ньому, та її захворювання. У програму інтегровано модель convnext_tiny_fp32_litert.tflite, яка мала найвищі показники точності за підсумками навчання. Як можна побачити на рис.11, програма демонструє користувачу найбільш імовірний клас зображення та його опис, після чого наводить перелік з топ-5 найімовірніших класів, до яких може належати зображення, та відсоток імовірності його приналежності до кожного класу. У випадку, зображеному на рис.11, зображення було класифіковано коректно – модель призначила найбільший відсоток імовірності правильному класу. Якщо правильний клас опинився на другому-п’ятому місці серед топ-5 найімовірніших класів, користувач може натиснути на його назву і тоді сторінка оновиться і демонструватиме опис та поради саме для обраного класу. За бажанням користувач може зберегти рослину та її діагноз, натиснувши на кнопку «Save to My Plants». Збереження рослини доступне лише для зареєстрованих користувачів. Зображення зберігається саме з тим класом, який визначив користувач (за замовчуванням – це клас з найбільшою ймовірністю.

4 Висновки

У результаті дослідження можна зазначити, системи ідентифікації захворювань рослин за допомогою алгоритмів машинного навчання» було здійснено певний комплекс заходів задля досягнення головної мети роботи. По-перше, було проаналізовано деякі теоретичні аспекти предметної області, серед яких: існуючі ризики для врожаїв, захворювання рослин як один з найсерйозніших викликів у сфері сільського господарства, традиційні способи виявлення хвороб та їхні недоліки, а також існуючі програмні рішення для подолання недоліків традиційних підходів. Цей крок дозволив з'ясувати, що захворювання рослин призводять до серйозних втрат врожаїв та прибутку, а методи ручного чи лабораторного виявлення хвороб не завжди є ефективними та доступними, тому актуальність застосування технологій машинного навчання та штучного інтелекту в цій сфері є високою. По-друге, було оглянуто існуючі інтелектуальні підходи для аналізу зображень, серед яких згорткові нейронні мережі та візуальні трансформери. Серед конкретних проаналізованих архітектур – EfficientNet-B0, MobileNetV3-Small, ResNet-18, YOLOv8n-cls, DenseNet-121, ConvNeXt-Tiny та MobileViT-XXS. Проведений аналіз показав, що всі ці моделі характеризуються високою здатністю до розпізнавання об'єктів та низьким рівнем обчислювальних витрат, що робить їх ідеальними варіантами для застосування у мобільних системах. Остання задача складалася з двох етапів – тренування моделей нейронних мереж та розробка мобільного застосунку. Навчання моделей відбувалося на двох різних наборах даних – PlantVillage (лабораторні фото) і PlantWild (польові знімки). Під час першого етапу тренування на PlantVillage усі моделі досягли високої точності, а на PlantWild точність дещо знизилася через більшу складність зображень. Модель, яка показала найвищий рівень точності (ConvNeXt-Tiny), було інтегровано у мобільний застосунок. Мобільну програму було розроблено з використанням сучасного стеку технологій – було використано мову Kotlin, середовище розробки Android Studio, бібліотеки Jetpack Compose для побудови інтерфейсу і TensorFlow Lite Interpreter для роботи з моделлю нейронної мережі, а також базу даних Room для збереження користувацьких даних профілю, налаштувань та рослин. Ці технології допомогли розробити застосунок, який характеризується низькими обсягами обчислювальних витрат, легкістю використання та високою швидкістю роботи.

В майбутньому систему можна буде розвинути, провівши пошук і застосування заходів для підвищення точності моделей, які можуть використовуватися в системі, та навчання на наборах даних з більшою кількістю класів, щоби застосунок допомагав користувачам працювати з більшою кількістю культур та захворювань.

Література

[1] Chornobay L., Mushenyk I. Modern Risks of Agricultural Activity and Methods of Their Leveling. Modern Economics. – 2023. – Vol. 42. – PP. 111–116.: DOI: https://doi.org/10.31521/modecon.V42(2023)-16.

[2] Agrios G. N. Plant Pathology. – 5th ed. – Academic Press, 2005: DOI: https://doi.org/10.1016/C2009-0-02037-6.

[3] Tan M., Le Q. V. EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. – Proceedings of the 36th International Conference on Machine Learning. – 2019. – Vol. 97. – PP. 6105–6114: https://proceedings.mlr.press/v97/tan19a.html

[4] Howard A., Sandler M., Chu G., Chen L.-C., Chen B., Tan M., Wang W., Zhu Y., Pang R., Vasudevan V., Le Q. V., Adam H. Searching for MobileNetV3. – Proceedings of the IEEE/CVF International Conference on Computer Vision. – 2019.–PP.1314–1324.URL: https://openaccess.thecvf.com/content_ICCV_2019/html/Howard_Searching_for_Mobile NetV3_ICCV_2019_paper.html.

[5] He, K., Zhang, X., Ren, S. and Sun, J. (2016) Deep Residual Learning for Image Recognition. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, 27-30 June 2016, 770-778. https://doi.org/10.1109/CVPR.2016.90

[6] Huang, G., Liu, Z., Van Der Maaten, L. and Weinberger, K.Q. (2017) Densely Connected Convolutional Networks. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Honolulu, 21-26 July 2017, 4700-4708. https://doi.org/10.1109/CVPR.2017.243

[7] Liu, Z., Mao, H., Wu, C., Feichtenhofer, C., Darrell, T. and Xie, S. (2022) A ConvNet for the 2020s. 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), New Orleans, 18-24 June 2022, 11966-119760. https://doi.org/10.1109/cvpr52688.2022.01167

[8] Mohanty S. P., Hughes D. P., Salathé M. Using Deep Learning for Image-Based Plant Disease Detection. Frontiers in Plant Science. – 2016. – Vol. 7. – Article 1419.: DOI: https://doi.org/10.3389/fpls.2016.01419

[9] Wei T., Chen Z., Huang Z., Yu X. Benchmarking In-the-wild Multimodal Disease Recognition and A Versatile Baseline. – Proceedings of the 32nd ACM International Conference on Multimedia. – 2024. – PP. 1593–1601.: https://doi.org/10.1145/3664647.3680599.

[10] Dong X., Zhao K., Wang Q., et al. PlantPAD: a platform for large-scale image phenomics analysis of disease in plant science. Nucleic Acids Research. – 2024. – Vol. 52, Issue D1. – PP. D1556–D1568.: https://doi.org/10.1093/nar/gkad917.

[11] Wei T., Chen Z., Yu X., Chapman S., Melloy P., Huang Z. A Large-Scale In-the-wild Dataset for Plant Disease Segmentation. Scientific Data. – 2026. – Vol. 13. – Article 205.: https://doi.org/10.1038/s41597-025-06513-4

[12] Singh D., Jain N., Jain P., Kayal P., Kumawat S., Batra N. PlantDoc: A Dataset for Visual Plant Disease Detection. – Proceedings of the 7th ACM IKDD CoDS and 25th COMAD. – 2020. – PP. 249–253. DOI: :https://dl.acm.org/doi/proceedings/10.1145/3371158

[13] Alvaro Fuentes, Sook Yoon, Sang Kim, and Dong Park. 2017. A robust deep-learning-based detector for real-time tomato plant diseases and pests recognition. Sensors 17, 9 (2017), 2022.:https://doi.org/10.3390/s17092022.

[14] Dong X., Zhao K., Wang Q., et al. PlantPAD: a platform for large-scale image phenomics analysis of disease in plant science. Nucleic Acids Research. – 2024. URL: https://doi.org/10.1093/nar/gkad917.

[15] ConvNeXt-based anchor-free object detection model for infrared image of power equipment / Zhang Y., et al. // Energy Reports. – 2023. – 9(7). C. 1121–1132.: https://doi.org/10.1016/j.egyr.2023.04.145.

[16] S. Khankalantary, M. Eskandar, Dual-stage parameter-efficient tuning for in-field plant disease few-shot classification 248 (2026).: https://doi.org/10.1016/j.compag.2026.111691.

[17] Y. Chu , D. Jiang, Y. Rao, Y. Zhang, Z. Fu, J. Yang. A dataset of multimodal tomato disease detection (2026) https://doi.org/10.11922/11-6035.csd.2026.0008.zh

INTELLIGENT SYSTEM FOR PLANT DISEASE IDENTIFICATION FROM IMAGES BASED ON DEEP LEARNING

Dr.Sci., Antoshchuk S., Ph.D., Kunup T., Kravchenko O.
Odessa Polytechnic National University, Ukraine

Abstract. This article presents a comprehensive study on the development of a plant disease identification system using machine learning algorithms. The aim of the work is to automate the process of identifying plant diseases based on visual appearance. The primary objective is to develop intelligent software capable of rapidly and accurately analyzing a plant's condition from a photograph. All aspects of developing the image-based plant disease identification system have been defined and implemented. Existing software products used for plant health assessment were analyzed to identify their strengths and weaknesses, and detailed requirements regarding the system's functionality and quality characteristics were established. Particular attention was paid to convolutional neural networks (CNNs) - specifically their image processing and feature extraction principles, as well as various architectures. Several network models were trained on the PlantVillage and PlantWild datasets to compare their accuracy. The developed system utilizes the model that achieved the highest percentage of correct predictions on the PlantDoc test dataset. The plant disease identification software was implemented as a mobile application. The study's relevance is underscored by the fact that, throughout the history of agriculture, humanity has faced numerous challenges in successfully preserving crops; plant diseases caused by various hazardous factors represent one of the most significant of these problems. Today, modern technologies help simplify and improve operations across many sectors, and agriculture is no exception. The system developed as part of this project serves as an easy-to-use tool for rapidly assessing plant health, enabling farm workers to take timely and effective measures to save their crops.

Keywords: *image classification, plant disease identification, convolutional neural networks, deep learning, PlantVillage, PlantWild, PlantDoc, artificial intelligence.*

УДК 544.18:004.85
DOI

МЕЖІ ТОЧНОСТІ ПОТЕНЦІАЛІВ МАШИННОГО НАВЧАННЯ ДЛЯ ДЕФЕКТІВ І ЛЕГУВАННЯ ГРАФЕНОВИХ КВАНТОВИХ ТОЧОК

Тужиков А.[1][0009-0005-3853-9911], Dr.Sci., Соловйов В.[1,3][0000-0002-4945-202X], Dr.Sci., Ків А.[2][0000-0002-0991-2343], Бєлінський А.[4][0000-0002-2821-2895]

[1]Державний заклад «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Україна,
[2]Університет імені Бен-Ґуріона в Негеві, Ізраїль,
[3]Київський національний економічний університет імені Вадима Гетьмана, Україна,
[4]Державний університет економіки та технологій, Україна
EMAIL:andrewtuzhykov@gmail.com

Анотація. *Потенціали машинного навчання (MLIP) дедалі частіше заміняють теорію функціонала густини (DFT), коли треба перебрати сотні структур. Але вони систематично занижують енергію структур, далеких від рівноваги. Досі не було зрозуміло, від чого залежить це заниження і коли такій моделі можна довіряти. Мета полягає у знаходжені структурної ознаки, яка визначає похибку універсального MLIP. У роботі порівняно універсальний потенціал SevenNet зі спін-поляризованим DFT (GPAW, PBE) на коронені $C_{24}H_{12}$. Кожну структуру релаксують один раз, а обидва методи оцінюють ту саму геометрію за однією формулою. На 28 конфігураціях вакансій і дивакансій потенціал завжди занижує енергію утворення: від 0,299 еВ для вакансії з цілим краєм до 1,112 еВ для дивакансії з двома розірваними зв'язками C–H, тобто на 0,2–0,4 еВ на кожен розірваний зв'язок. Поворот Стоуна–Уельса, який не розриває зв'язків, відтворюється з точністю 0,013 еВ. Для легування азотом розходження з DFT не перевищує 0,068 еВ, а для B, O, S і S_i зсув однаковий для всіх позицій елемента, тобто його визначає резервуар, а не позиція. Отже, придатність потенціалу визначає число розірваних зв'язків у структурі, а не точність моделі загалом. Разом із розкидом енергії всередині класу симетрії та перевіркою топології позиції це дає три прості правила для автоматичного конвеєра, у якому попередній відбір xTB → MLIP триває секунди, а DFT, що потребує годин, залучають лише для відібраних кандидатів.*

Ключові слова: *графенова квантова точка, точковий дефект, легування заміщенням, теорія функціонала густини, сурогатна модель, потенціали машинного навчання, SevenNet, систематичне пом'якшення, валідація моделі, коронен, агентні системи, енергія утворення.*

1 Вступ

Постановка проблеми. Графенові квантові точки (ГКТ) - це фрагменти графену розміром у кілька нанометрів. На відміну від нескінченного листа, вони мають край і енергетичну щілину, яку можна змінювати розміром і формою фрагмента. Тому їх розглядають як матеріал для електродів накопичувачів енергії, безметалевих каталізаторів і флуоресцентних міток [1]. Робочі властивості таких фрагментів визначає не ідеальний каркас, а дефекти. Їх три головні типи. Вакансії - вилучені атоми вуглецю, після яких каркас перебудовується і може лишити неспарені електрони. Перебудови краю - повороти зв'язків, які перетворюють шестикутники на пари п'ятикутник–

семикутник без зміни складу. Гетероатоми, введені заміщенням, — B, N, O, P, S або Si на місці атома вуглецю; вони змінюють спектр і хімічну активність фрагмента, не руйнуючи каркаса [2]. Щоб спроєктувати ГКТ із потрібними властивостями, треба перебрати сотні таких конфігурацій: кожен тип дефекту, кожна позиція на фрагменті й кожен розмір фрагмента дають окрему структуру. Теорія функціонала густини (DFT) у формулюванні Кона–Шема [3] лишається основним еталонним методом для таких задач, але її вартість росте приблизно як куб числа атомів. Систематичний перебір конфігурацій навіть для молекули з тридцяти атомів триває багато діб. У праці авторів [4] розглянуто, як методи штучного інтелекту доповнюють методи ab initio і де саме їхня вартість стає перепоною для проєктування матеріалів. Саме цей розрив між потрібним масштабом і доступною вартістю і покликані закрити сурогатні моделі.

Аналіз останніх досліджень і публікацій. Потенціали машинного навчання (MLIP) є такими сурогатами. Ідею запропонували Белер і Парінелло: енергію системи подають як суму внесків атомів, а внесок кожного атома обчислює нейронна мережа за його оточенням [5]. Перші потенціали описували оточення фіксованими ознаками, як-от ґаусові апроксимаційні потенціали (GAP) [6]. Еквіваріантні графові мережі NequIP [7] і MACE [8] самі навчаються представлень оточення й досягають точності DFT на тисячах конфігурацій замість сотень тисяч. Далі з'явилися універсальні моделі, навчені на даних для більшої частини періодичної системи, серед них M3GNet [9] і SevenNet [10]. Їх пропонують як готовий інструмент, який не треба донавчати під конкретну систему. Ціна універсальності відома. На матеріалах з бази Materials Project показано [11], що три поширені універсальні MLIP (M3GNet, CHGNet і MACE-MP-0) систематично недооцінюють кривизну поверхні потенціальної енергії і, як наслідок, енергії конфігурацій, далеких від рівноваги. Це явище назвали систематичним пом'якшенням (systematic softening). Причина в навчальних даних: у них переважають структури поблизу мінімумів енергії з траєкторій релаксації, тож модель рідко бачить круті ділянки поверхні потенціальної енергії. Для наноструктур із краями можна очікувати, що ця вада буде сильнішою, ніж для кристалів. Крайовий атом ГКТ із розірваним зв'язком поводиться як молекулярний радикал, а не як дефект у ґратці. Самі перебудови краю добре вивчені методами DFT: відомі самопасивувальні реконструкції [12], перехід зигзагу в мотив 5–7 [13] і кутові стани зигзагових стрічок [14]. Ці роботи описують, що відбувається на краю, але не кажуть, з якою похибкою це відтворює сурогат. Порівняння сурогату з DFT раніше зроблено для орієнтаційних дефектів у полімерах [15], і там питання про залежність похибки від типу конфігурації теж лишилося відкритим. Для пірену $C_{16}H_{10}$, найменшого фрагмента з усіма трьома типами дефектів, автори порівняли обидва методи за всіма позиціями [16]. Картина вийшла контрастною: повороти Стоуна–Уельса потенціал відтворив із похибкою 0,06 еВ, центральні вакансію й дивакансію занизив на 0,63 і 0,59 еВ, а на крайових дивакансіях розійшовся з DFT на 4–5 еВ, бо зійшовся до іншої структури. Саме цей контраст і став відправною точкою цієї роботи.

Невирішені раніше частини загальної проблеми. Отже, невідомо, як пом'якшення залежить від типу конфігурації. Опубліковані оцінки подають

похибку одним числом для всієї моделі. З такого числа не видно, коли потенціалу можна довіряти, а коли ні. Потрібна ознака, яку видно зі структури ще до розрахунку і яка передбачає похибку. Є й методична прогалина, яку показав приклад пірену [16]. Зазвичай DFT і MLIP порівнюють за двома незалежними релаксаціями. Для крайових позицій з кількома мінімумами вони можуть зійтися до різних структур, і тоді різниця енергій змішує похибку моделі з різницею структур. Нарешті, для легування опубліковані розрахунки беруть один розмір фрагмента й лише кілька положень домішки (у [2] — три). З них не видно, що в результаті залежить від елемента, а що від конкретного фрагмента.

Мета статті - знайти структурну ознаку, яка визначає похибку універсального MLIP у ГКТ, і виміряти цю залежність так, щоб обидва методи оцінювали ті самі структури. Для цього поставлено такі завдання: виміряти похибку потенціалу для трьох точкових дефектів коронену (моновакансія, дивакансія, поворот Стоуна–Уельса) на парних конфігураціях з однаковою геометрією та однаковими резервуарами; перевірити, чи визначає похибку число розірваних крайових зв'язків C–H, а не тип дефекту; виміряти похибку для заміщення вуглецю на *B, N, O, P, S*$_i$, де число зв'язків не змінюється; з'ясувати, чи зберігає потенціал правильний порядок конфігурацій там, де він помиляється в абсолютних значеннях; записати критерій придатності у вигляді правил для автоматичного конвеєра й показати, як він працює в агентній системі.

Частину результатів щодо дефектів коронену викладено в статті [17]. Тут їх подано українською, доповнено легуванням шістьма домішками і розглянуто разом із конвеєром автоматизації, чого у статті [17] не було.

2 Системи, методи та протокол порівняння

Усі розрахунки виконано на родині фрагментів графену з повністю насиченими воднем краями (рис. 1, табл. 1).

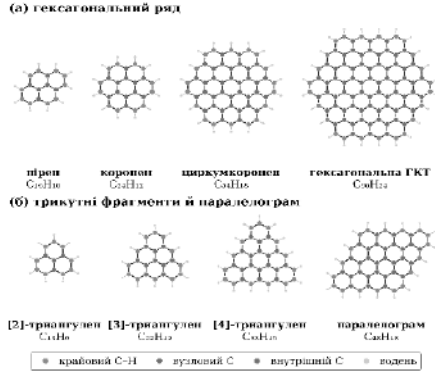


Рисунок 1. Родина фрагментів графену, на яких порівнюються методи, у спільному масштабі; атоми вуглецю розфарбовано за класом позиції: (а) гексагональний ряд від пірену до $C_{96}H_{24}$; (б) [2, 3, 4]-триангулени й паралелограм $C_{48}H_{18}$

Головна модельна система - коронен $C_{24}H_{12}$, гексагональна ГКТ із симетрією D_{6h}. У ній лише три класи атомів вуглецю: крайовий, що несе водень

(12 атомів), вузловий без водню на стику двох кілець (6) і внутрішній на стику трьох кілець (6). Кожен клас тут збігається з однією орбітою симетрії. Мала кількість класів зручна для контролю: за симетрією всі позиції одного класу мусять мати однакову енергію утворення. Якщо розкид усередині класу великий, релаксація зійшла до різних структур. Решта фрагментів потрібна, щоб відокремити властивості класу позиції від властивостей конкретної молекули. Гексагональний ряд продовжує коронен в обидва боки. Пірен $C_{16}H_{10}$ менший за нього, циркумкоронен $C_{54}H_{18}$ більший у 2,25 раза, а $C_{96}H_{24}$ - у чотири. Усі вони мають той самий набір трьох класів (число орбіт симетрії див. у табл. 1).Від пірену до циркумкоронену число атомів вуглецю зростає більш як утричі, тому саме на цих трьох фрагментах перевіряється переносність легування, а шість орбіт циркумкоронену дають профіль енергії вглиб. Трикутні фрагменти - [2, 3, 4]-триангулени $C_{13}H_9$, $C_{22}H_{12}$ і $C_{33}H_{15}$ із симетрією D_{3h} - мають інше оточення внутрішніх позицій і неспарені електрони вже без дефектів: [n]-триангулен несе їх n − 1, і DFT для [4]-триангулену справді знаходить три. Паралелограм $C_{48}H_{18}$ (D_{2h}) додає фрагмент із гострими кутами.

Таблиця 1

Модельні системи: симетрія, число атомів вуглецю кожного класу (крайових C–H, вузлових, внутрішніх), число орбіт симетрії та роль у роботі

Фрагмент	Симетрія	C–H / вузл. / внутр.	Орбіт	Роль у роботі
Пірен $C_{16}H_{10}$	D2h	10 / 4 / 2	5	легування: менший фрагмент
Коронен $C_{24}H_{12}$	D6h	12 / 6 / 6	3	головна система: карти дефектів, легування, порівняння методів
Циркумкоронен $C_{54}H_{18}$	D6h	18 / 12 / 24	6	легування, профіль вглиб, ряд розмірів
Гексагональна ГКТ $C_{96}H_{24}$	D6h	24 / 18 / 54	10	межа розміру, перевірка структури позицій
[2]-триангулен $C_{13}H_9$	D3h	9 / 3 / 1	4	ряд розмірів
[3]-триангулен $C_{22}H_{12}$	D3h	12 / 6 / 4	6	ряд розмірів
[4]-триангулен $C_{33}H_{15}$	D3h	15 / 9 / 9	8	ряд розмірів, перевірка наближених методів
Паралелограм $C_{48}H_{18}$	D2h	18 / 12 / 18	14	форма проти розміру

Розрахунки DFT виконано пакетом GPAW (grid-based projector-augmented wave) [18] через інтерфейс ASE [19]. Використано функціонал PBE (Perdew–Burke–Ernzerhof) [20] зі спіновою поляризацією. Для карт дефектів взято

плоскохвильове відсікання 400 еВ, комірку 15 Å і релаксацію BFGS до сили 0,05 еВ/Å у точці Г. Для легування параметри посилено: відсікання 600 еВ, комірка за розміром молекули, розмиття Фермі–Дірака 0,02 еВ з фіксованим магнітним моментом, релаксація до 0,02 еВ/Å. Причина проста: хімічний потенціал азоту між 400 і 600 еВ змінюється на 1,65 еВ, а $C_{23}NH_{12}$ зі 157 електронами є дублетом, і при розмитті 0,05 еВ розрахунок збігався до хибного нульового моменту.

Потенціал - SevenNet [10], модель 7net-omni-i12 (SevenNet-Omni [21]). Вона має кілька вихідних голів (heads), навчених на різних наборах даних і різних рівнях теорії. Карти дефектів і повороти Стоуна–Уельса розраховано головою за замовчуванням (mpa, рівень PBE(+U)) у комірці 30 Å з тим самим критерієм сил, що й у DFT. Легування і ряд фрагментів розраховано головою omol25_high, навченою на молекулярних розрахунках ωB97M-V для високоспінових конфігурацій [21]. Ці два набори чисел не лежать на одній шкалі, тому їх ніде не порівнюють між собою напряму. Оскільки еталоном є PBE, розходження голови omol25_high з DFT містить не лише похибку навчання, а й різницю функціоналів ωB97M-V і PBE. Кожен блок результатів зіставляють лише зі своєю DFT-стороною. Для ряду фрагментів (підрозділ 3.5) і порівняння методів (розділ 5) використано ще DFT у гаусовому базисі PySCF/PBE [22], def2-SVP [23] і напівемпіричний метод GFN2-xTB [24].

Енергію утворення дефекту й енергію заміщення розраховували за однією формулою через зміну складу:

$$E_f = E(\textit{дефект}) - E(\textit{ідеал}) - \sum_i \Delta n_i \mu_i , \qquad (1)$$

де Δn_i - зміна числа атомів сорту i, μ_i - хімічний потенціал його резервуара. Сума береться по всіх елементах. Це важливо: піридинова конфігурація змінює одразу вуглець, водень i азот, і формула лише для двох елементів втратила б член $-\mu_N$. Резервуари: графен для вуглецю, $H_2/2$ для водню, $N_2/2$ для азоту, $O_2/2$ для кисню, молекула P_4 (білий фосфор) для фосфору, циклічна молекула S_8 для сірки, диборан B_2H_6 для бору й силан SiH_4 для кремнію. Хімічні потенціали обчислює той самий метод, що й структури. Інакше не скоротився б довільний нуль енергії, який для голови omol25_high становить близько −1037 еВ на атом вуглецю (повна енергія з урахуванням остовних електронів), а для GPAW і голови mpa - близько − 9 еВ (для карт дефектів $\mu_C = -8{,}861$ і $\mu_H = -3{,}355$ еВ у DFT проти − 9,221 і −3,364 еВ у MLIP).

Головний прийом роботи - парне порівняння. Кожну структуру релаксують один раз, а потім ту саму геометрію оцінюють обидва методи за формулою (1) зі своїми резервуарами. Так із різниці зникає внесок різних геометрій, і лишається лише різниця самих поверхонь потенціальної енергії.

Конфігурації будували повним перебором за орбітами симетрії. Для дефектів почергово вилучали кожен атом вуглецю (моновакансія) і кожну пару сусідніх атомів (дивакансія) та повертали кожен зв’язок на 90° (Стоун–Уельс); кожен варіант релаксували окремо. Так отримано повні карти енергій, а з них 28 парних конфігурацій. Для легування перебирали орбіти симетрії кожного

фрагмента і розрізняли графітне заміщення в глибині та крайове X–H на ободі. Глибину позиції міряли відстанню до найближчого крайового атома вуглецю.

3 Дефекти: похибка росте з числом розірваних зв'язків

3.1 Поворот Стоуна–Уельса: зв'язки цілі, потенціал точний

Поворот Стоуна–Уельса не змінює ні числа атомів, ні числа зв'язків. Обертання одного зв'язку C–C на 90° перетворює чотири шестикутники на два п'ятикутники й два семикутники, а біля краю — на пару п'ятикутник–семикутник. Структура лишається близькою до рівноваги, і саме тут потенціал найточніший. На тридцяти таких поворотах середня енергія утворення становить 1,891 еВ за DFT і 1,878 еВ за MLIP. Розходження 0,013 еВ (табл. 2) найменше серед усіх класів і на порядок менше за похибки для вакансій. Цей рядок таблиці важливіший за саме число: пом'якшення виникає не для будь-якого дефекту, а лише для певного класу конфігурацій. Одне застереження стосується автоматичних карт. Там поворот крайового зв'язку іноді відриває атом, і карта насичує його воднем. У парному протоколі такого немає, бо склад обох сторін однаковий за побудовою.

Таблиця 2

Похибка потенціалу за класами дефектів коронену: середні енергії утворення для парних конфігурацій з однаковою геометрією та однаковими резервуарами

Дефект	Розірваних C–H	n	DFT, еВ	MLIP, еВ	δ = MLIP − DFT, еВ
Стоун–Уельс	0	30	1,891	1,878	−0,013
Моновакансія	0	2	1,808	1,509	−0,299
Моновакансія	1	4	2,497	1,758	−0,739
Дивакансія	0	17	1,139	0,487	−0,653
Дивакансія	1	2	4,593	3,737	−0,856
Дивакансія	2	3	5,798	4,686	−1,112

3.2 Похибка росте з числом розірваних крайових зв'язків

На 28 парних конфігураціях вакансій і дивакансій потенціал занижує енергію утворення в кожному випадку. Заниження не є сталим. Для вакансії в глибині, де край цілий, воно становить 0,299 еВ. Для дивакансії з цілим ободом - 0,653 еВ. Для дивакансії, яка розриває два крайові зв'язки C–H, - 1,112 еВ. Якщо впорядкувати конфігурації за числом розірваних зв'язків C–H, а не за типом дефекту, заниження монотонно зростає (рис. 2): кожен розірваний зв'язок додає 0,44 еВ для моновакансій і 0,20–0,26 еВ для дивакансій, тобто 0,2–0,4 еВ на зв'язок. Число розірваних зв'язків важить більше, ніж тип дефекту. Моновакансія з одним розірваним зв'язком (0,739 еВ) ближча до дивакансії з одним розірваним зв'язком (0,856 еВ), ніж до моновакансії з цілим краєм (0,299 еВ). Проте й тип дефекту має значення: за цілого краю дивакансія має вдвічі більше заниження, ніж моновакансія (0,653 проти 0,299 еВ).

Причина узгоджується з поясненням пом'якшення через навчальні дані [11]. Розірваний крайовий зв'язок лишає атом вуглецю з неспареним електроном. Таких радикальних структур у навчальній вибірці з релаксованих кристалів майже немає.

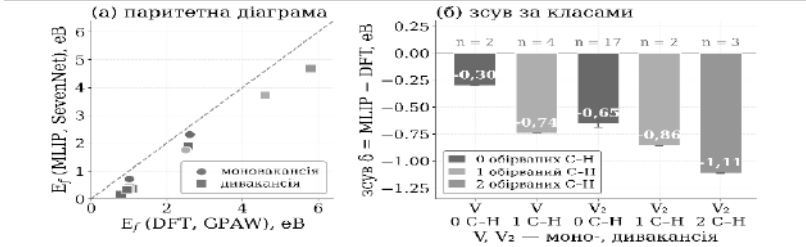


Рисунок 2. Систематичне пом'якшення потенціалу на 28 парних конфігураціях: (а) паритетна діаграма енергій утворення MLIP проти DFT, усі точки лежать нижче лінії ідеальної відповідності; (б) похибка δ = MLIP − DFT залежно від числа розірваних крайових зв'язків С–Н, 0,2–0,4 еВ на зв'язок

Частину цієї енергії можна назвати точно: для вузлової моновакансії коронену спін-поляризований DFT знаходить стан на 0,372 еВ нижчий, ніж розрахунок із мінімальною мультиплетністю, яку задає парність числа електронів. Потенціал спіну не має за побудовою, тож цієї енергії в ньому немає. Практичний висновок простий: число розірваних зв'язків видно зі структури, тому поправку можна вводити наперед.

3.3 Затиснутий водень задає структуру дефекту

Один і той самий дефект рідко відповідає одній структурі. Вирізання крайової дивакансії лишає два атоми вуглецю з розірваними зв'язками один навпроти одного. Що буде далі, залежить від того, чи є чим їх наситити. Якщо водню немає, ці атоми зв'язуються між собою, і порожнина стягується в пару п'ятикутників: непасивована дивакансія по зв'язку застигає в мотиві 5–5 з енергією 5,80 еВ. Якщо водень є, він насичує кожен із цих атомів, зв'язок С–С не утворюється, і край лишається рядом шестикутників з енергією 0,77 еВ. Проміжний стан з одним насиченим атомом дає один п'ятикутник з енергією 2,56 еВ. Отже, кожен п'ятикутник потребує в середньому близько 2,5 еВ.

Для потенціалу тут важливо інше. Він занижує кожне з цих значень, але розташовує три структури в тому самому порядку, що й DFT, і зберігає великі проміжки між ними. Тому пошук структур із потенціалом як фільтром вибере правильну структуру, хоча й повідомить для неї неправильну енергію. Це похибка калібрування, а не розрізнення. З такою похибкою можна працювати, якщо потенціал відбирає кандидатів, а DFT ухвалює остаточне рішення.

3.4 Симетрія показує ненадійні позиції, але не доводить правильності

Парне порівняння вимагає, щоб обидва методи оцінювали ту саму структуру. Як автоматичний конвеєр, що релаксує кожну позицію окремо, дізнається, що ця умова порушилася? Першу відповідь дає симетрія. За симетрією D_{6h} усі позиції одного класу мусять мати однакову енергію. Отже, розкид усередині класу є сигналом похибки, який дістається безкоштовно. Потенціал повертає одне значення на клас: розкид ніде не перевищує 0,002 еВ. DFT зі спіновою поляризацією зберігає симетрію для класів із замкненою оболонкою, але грубо порушує її для шести однакових вузлових атомів. Незалежно релаксовані моновакансії на них розкидані на 5,85 еВ (від 0,13 до 5,98 еВ), а на внутрішньому класі розкид сягає 1,76 еВ.

Це не фізичний ефект, бо позиції справді однакові. Так поводиться оптимізатор без обмежень: він сідає в різні структури з підрозділу 3.3 залежно від числових випадковостей. Вузловий атом коронену є молекулярним аналогом кута зигзагового краю. Такі краї нестійкі до перебудови [12], переходять у мотиви 5–7 [13] і мають кутові стани [14]. Саме між цими конкурентними структурами оптимізатор і вибирає навмання. Тому великий розкид усередині класу вказує на позиції, для яких «число з DFT» просто не визначене однозначно, і робить це ще до будь-якого порівняння методів.

Але в цього індикатора є межа, яку показали більші фрагменти: малий розкид доводить повторюваність, а не правильність. Внутрішня моновакансія має перебудовуватися в мотив 5–9. В автоматичних картах голова за замовчуванням замість нього дала складений мотив 5–5 або взагалі неперебудоване 12-членне кільце на 2 із 12 внутрішніх позицій $C_{54}H_{18}$ і на 6 із 20 позицій $C_{96}H_{24}$ (на коронені всі 6 позицій були правильні). GFN2-xTB помилявся на 10 із 20 позицій $C_{96}H_{24}$. При цьому розкид усередині орбіти в хибних картах становив лише 0,02–0,04 еВ, тобто карта виглядала цілком узгодженою. Помилку виявляє лише окрема перевірка структури позиції: числа кілець навколо неї і виходу каркаса з площини. Ця перевірка знайшла хиби в кожному методі, і жодну з них не було видно за енергіями.

3.5 Розмір і форма фрагмента

Чи залежить виміряна похибка від коронену, чи від класу конфігурації? На це відповідає ряд фрагментів. Різниця енергій вузлової та глибинної вакансій не містить резервуарів, тож її можна порівнювати між методами без застережень. На ряду від [2]-триангулену $C_{13}H_9$ до циркумкоронену $C_{54}H_{18}$ похибка потенціалу (omol25_high) відносно DFT PySCF/PBE на однакових геометріях становить у середньому 0,133 еВ, найбільше 0,252 еВ, і її знак чергується (рис. 3, а). Ця величина містить і різницю функціоналів ωB97M-V і PBE (розділ 2), тож не є чистою похибкою навчання. Похибка не росте з розміром. Еталон при цьому надійний: GPAW і PySCF дають для пари 5–7 коронену 1,606 і 1,624 еВ, тобто розходяться лише на 0,018 еВ.

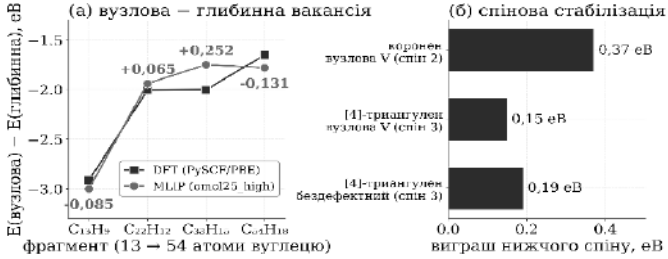


Рисунок 3. Ряд фрагментів від $C_{13}H_9$ до $C_{54}H_{18}$: (а) різниця енергій вузлової та глибинної вакансій за MLIP (omol25_high) і DFT (PySCF/PBE, def2-SVP) на однакових геометріях, підписано похибку потенціалу; (б) спінова стабілізація, яку знаходить DFT і якої потенціал не має за побудовою

Форма важить більше за розмір. У ряду $C_{24} \rightarrow C_{54} \rightarrow C_{96}$ енергія крайової вакансії монотонно спадає (1,409 → 0,728 → 0,626 еВ за головою omol25_high), а глибинна виходить на плато вже при C_{54}: 6,50 і 6,47 еВ різняться лише на 0,03

еВ. Тобто вплив краю на глибинну вакансію вичерпується вже у фрагменті з 54 атомів вуглецю. Водночас та сама глибинна вакансія потребує 5,7–6,5 еВ у гексагональних точках і лише 2,9–3,9 еВ у триангуленах і паралелограмі такого самого розміру. Отже, енергію вакансії визначає оточення позиції, тобто форма фрагмента, а не його розмір.

4 Легування: заміщення без розриву зв'язків

4.1 Навіщо потрібне легування

Поворот Стоуна–Уельса - лише один тип конфігурації без розірваних зв'язків. Заміщення атома вуглецю на гетероатом дає незалежну перевірку: хімія позиції змінюється сильно, а число зв'язків лишається тим самим. Якщо критерій правильний, потенціал має бути точним і тут. Числа цього розділу розраховано головою omol25_high, а в розділі 3 працювала голова за замовчуванням mpa (рівні теорії ωB97M-V і PBE відповідно). Ці набори не лежать на одній шкалі, тому далі порівнюємо не абсолютні значення двох розділів, а лише розходження кожного з них зі своїм DFT.

4.2 Енергія заміщення в коронені

Для шести домішок (B, N, O, P, S і Si) розраховано три конфігурації від ободу вглиб: крайову X–H, вузлову й центральну (табл. 3). DFT-сторону розраховано GPAW із посиленими параметрами (PW 600 еВ, fmax 0,02 еВ/Å, фіксований магнітний момент), MLIP-сторону головою omol25_high при fmax 0,1 еВ/Å. Обидві сторони використовують формулу (1) і резервуари розділу 2, кожна зі своїми хімічними потенціалами. За DFT для всіх домішок обід вигідніший за глибину. Зайняти крайову позицію, зберігши водень, потребує менше енергії, ніж стати графітним атомом усередині: для азоту різниця становить 0,587 еВ, для кисню 0,704 еВ, для кремнію 1,713 еВ. Два елементи випадають із ряду. У бору розмах за трьома орбітами усього 0,309 еВ. У кремнію крайова й вузлова позиції майже однакові (1,782 і 1,771 еВ), тобто його «поверхневий шар» на одну орбіту глибший, ніж у азоту й кисню.

Таблиця 3

Енергія заміщення вуглецю на гетероатом у коронені за орбітами симетрії: GPAW PW(600) / MLIP omol25_high, еВ, і зсув δ = MLIP − GPAW за трьома орбітами (крайову позицію кисню розраховано при fmax 0,05 еВ/Å, бо при 0,02 релаксація не збіглася)

Домішка	Крайова X–H	Вузлова	Центральна	δ, еВ
B	1,458 / 0,963	1,443 / 0,875	1,752 / 1,281	−0,57…−0,47
N	0,843 / 0,911	1,306 / 1,284	1,430 / 1,433	−0,02…+0,07
O	2,461 / 1,939	3,283 / 2,720	3,165 / 2,743	−0,56…−0,42
P	1,627 / 2,410	2,642 / 2,332	2,611 / 3,308	−0,31…+0,78
S	2,368 / 2,589	3,388 / 3,433	3,481 / 3,761	+0,05…+0,28
Si	1,782 / 2,032	1,771 / 2,159	3,495 / 3,770	+0,25…+0,39

На більшому фрагменті, циркумкоронені $C_{54}H_{18}$ із шістьма орбітами, це видно ще краще (рис. 4).

Профіль енергії вглиб має вигляд сходинки, а не плавного підйому: обід і перший шар лежать майже на одному рівні, потім різкий стрибок, потім плато. Для азоту й кисню сходинка стоїть між ободом і вузловим шаром (крок 0,672 і

1,250 еВ), для кремнію, фосфору й сірки на шар глибше (1,625, 0,930 і 0,695 еВ). Найпростіше пояснення структурне: Si, P і S більші за вуглець і мусять вийти з площини, а на вузловій орбіті каркас іще може прогнутися їм назустріч. Це лише гіпотеза, бо сірка не вписується в ряд за розміром, а позаплощинне зміщення окремо не перевіряли.

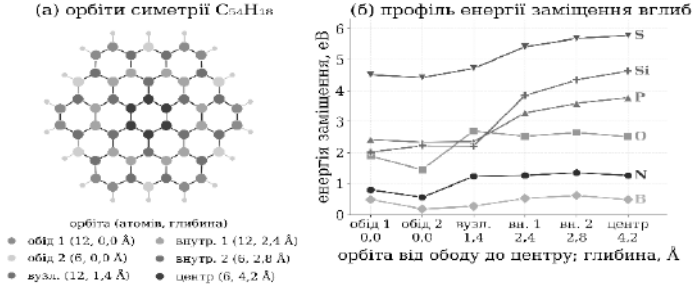


Рисунок 4. Профіль енергії заміщення вглиб циркумкоронену $C_{54}H_{18}$ за головою omol25_high: (а) шість орбіт симетрії від ободу до центру, у дужках число атомів в орбіті та глибина, тобто відстань до найближчого крайового атома вуглецю; (б) енергія прямого заміщення для шести домішок за тими самими орбітами. Для N і O сходинка стоїть між ободом і вузловою орбітою, для Si, P і S - на орбіту глибше, для B її немає

4.3 Керує глибина позиції, а не розмір точки

Порівнювати орбіти різних фрагментів за відстанню від центру не можна. У коронені орбіта з радіусом 3,74 Å складається з крайових атомів із воднем, а в циркумкоронені на тому самому радіусі лежать внутрішні атоми без водню. Правильна координата - відстань до найближчого крайового атома. За нею ряд $C_{16}H_{10} \rightarrow C_{24}H_{12} \rightarrow C_{54}H_{18}$ сходиться: при однаковій глибині розкид енергії заміщення не перевищує 0,170 еВ для азоту, 0,225 еВ для кисню, 0,227 еВ для фосфору й 0,359 еВ для кремнію, хоча число атомів вуглецю зростає більш як утричі. Два винятки різної природи: бор розходиться монотонно з розміром до 0,990 еВ, що схоже на чутливість до розміру π-системи, а сірка розходиться до 1,678 еВ немонотонно, що більше схоже на іншу релаксовану структуру.

4.4 Потенціал проти DFT там, де зв'язки цілі

Для азоту критерій підтверджується найкраще. Найбільше розходження за трьома орбітами становить 0,068 еВ, середнє +0,016 еВ, а на найглибшій позиції лише 0,003 еВ. Це порівнянно з точністю подання повної енергії у форматі float32 (≈0,002 еВ за повної енергії ~$2{,}5 \cdot 10^4$ еВ). Порядок орбіт 0,84 → 1,31 → 1,43 еВ відтворено точно (табл. 3). Для решти п'яти домішок картина інша, і саме вона уточнює критерій. Середнє абсолютне розходження по всіх 18 конфігураціях шести домішок становить 0,355 еВ. Але розподілене воно не за позиціями, а за елементами. Для бору зсув лежить у межах −0,57…−0,47 еВ на всіх трьох орбітах, для кисню −0,56…−0,42, для кремнію +0,25…+0,39, для сірки +0,05…+0,28. У межах елемента він майже сталий (табл. 3). Такий зсув є підписом резервуара. В E_f входить різниця $\mu_X - \mu_C$, і похибка потенціалу на еталонній молекулі домішки (диборан, силан, S_8) однаково переноситься в усі конфігурації цього елемента. Частина зсуву може походити від різниці рівнів

теорії (ωB97M-V у голови omol25_high проти PBE, який, зокрема, переоцінює енергію зв'язку O_2 приблизно на 1 еВ [20]); розділити ці внески можна лише порівнянням з ωB97M-V. Різниці між позиціями, у яких резервуар скорочується, потенціал відтворює: для B, N, O, S і Si розкид зсуву за орбітами не перевищує 0,24 еВ. Єдиний виняток - фосфор. Для нього потенціал міняє місцями крайову й вузлову позиції (+0,78 проти −0,31 еВ), і саме тут потрібна перевірка структури з підрозділу 3.4.

Дев'ятнадцять попередніх парних карт GPAW/MLIP на фрагментах C_6–C_{24} давали систематично від'ємний зсув: від −0,840 еВ для азоту до −0,572 для сірки. Але DFT там рахували при відсіканні 400 еВ, де Oj_N ще змінюється на 1,65 еВ, а MLIP - головою за замовчуванням. Той зсув був переважно похибкою постановки. Чинним із тих карт лишається ранжування: 17 карт із 19 дають ту саму найвигіднішу позицію, що й DFT. Із незалежними даними для нескінченного графену результати цієї роботи можна зіставити лише орієнтовно. Для кремнію значення цієї роботи 4,71–4,98 еВ після зведення резервуарів до графену й об'ємного кремнію вище як за оцінку дифузійного Монте-Карло (DMC) 4,4(1) еВ, так і за значення PBE 3,59–3,77 еВ [25]; частину різниці дають скінченний розмір і край фрагмента.

5 Агентний конвеєр: як застосувати критерій

Критерій із розділів 3 і 4 корисний лише тоді, коли його застосовує не людина вручну, а конвеєр. Рутинні етапи побудови й перевірки MLIP уже автоматизують агентні системи на великих мовних моделях, наприклад конвеєр AMLP, у якому агенти вибирають програму розрахунку, готують вхідні файли й обробляють вихідні [26]. Активне навчання додає до перебору оцінку невизначеності: модель сама надсилає конфігурацію на розрахунок DFT, коли невпевнена [27]. Слабке місце такої схеми в тому, що оцінка невизначеності є внутрішньою для моделі. Вона може бути надто впевненою саме там, де модель систематично зміщена. Результати цієї роботи дають зовнішні правила, які від моделі не залежать. Правил три, і всі вони читаються зі структури до розрахунку. Перше: число розірваних крайових зв'язків C–H передбачає заниження 0,2–0,4 еВ на зв'язок. Конфігурації без розірваних зв'язків розраховують лише потенціалом, а кожен розірваний зв'язок або додає поправку, або відправляє конфігурацію на DFT. Друге: розкид енергії всередині класу симетрії позначає позиції, для яких існує кілька структур. Третє, без якого перші два ненадійні: структуру релаксованої позиції (число кілець навколо неї, вихід каркаса з площини) перевіряють окремо від енергії, бо узгоджена карта може бути узгоджено хибною (підрозділ 3.4). Для легування є ще правило резервуара: абсолютні енергії заміщення несуть сталий для елемента зсув, тому конвеєр порівнює різниці між позиціями, а не абсолютні значення. Місце цих правил серед методів показує порівняння на одній задачі, парі 5–7 коронену (рис. 5, а). GFN2-xTB дає 1,672 еВ за 0,8 с, SevenNet (omol25_high) 1,87 еВ за 15 с, PySCF/PBE 1,624 еВ за 1,5 год, а еталон GPAW PW(600) 1,606 еВ за 4,3 год на одному потоці. Така ієрархія вигідна лише тоді, коли кожен рівень стартує з геометрії попереднього: старт DFT із геометрії потенціалу скоротив релаксацію з понад сорока кроків до дванадцяти. Де наближені методи відмовляють, видно на одинадцяти конфігураціях [4]-триангулену, звірених із

DFT (рис. 5, б, табл. 4). На ізомерах і вакансіях обидва наближені методи працюють, а на трьох внутрішніх моновакансіях з мотивом 5–9 обидва помиляються на 1,1–1,5 еВ. Вибір голови потенціалу теж є частиною правил. Голова за замовчуванням відтворює пару 5–7 коронену з точністю 0,06 еВ, але на C_{54} і C_{96} хибно перебудовує частину внутрішніх позицій. Голова omol25_high дає правильний мотив 5–9 всюди, зате завищує ту саму пару 5–7 на 0,27 еВ.

Таблиця 4

Середнє відхилення від DFT за типом задачі, еВ: що можна доручати наближеним методам

Тип задачі	n	GFN2-xTB	SevenNet	Придатність
Ізомери, склад не змінюється	4	0,025–0,066	0,145–0,265	висока
Вакансії, змінюються лише C і H	8	0,079	0,296	добра
Легування, відносні енергії	18	0,205	0,123	прийнятна
Легування, абсолютні E_f	18	1,419	0,355	відсутня
Вироджені позиції, щілина ≈ 0	3	1,321	1,150	відсутня

Агент, який виконує ці правила, складається з оркестратора й шести підагентів. Ролі розподілені не за етапами, а за типом відповідальності, бо кожна роль помиляється по-своєму. Агент переліку орбіт шукає симетрію на нерелаксованій геометрії й знаходить 33 орбіти замість восьми. Агент скринінгу видає геометрію, далеку від істинної, без жодної ознаки. Агент звітів підписує число з DFT під геометрією MLIP. Ключова роль - аудитор: набір перевірок перед кожним порівнянням двох чисел, який має право зупинити роботу. З одинадцяти його перевірок жодна не стосується квантової механіки. Кожна енергія несе метод, базис, розмиття, критерій сил і спін. E_f обчислює одна функція, а не людина. Ключ кешу містить усе, що змінює число. Розкид усередині орбіти друкується завжди. Закономірність потребує щонайменше трьох точок. Кожна з цих перевірок відповідає помилці, яка в цій роботі справді сталася. Конвеєр реалізовано на великій мовній моделі Claude Opus 5 (Anthropic) у середовищі Claude Code. Оркестратор - сесія моделі з доступом до файлів проєкту й інтерпретатора Python; підагенти — підзадачі з окремим контекстом, які повертають лише результат, тож помилка однієї не переходить у решту. Аудитор - набір скриптів Python, який від моделі не залежить і запускається перед кожним порівнянням двох чисел. Модель не рахує енергій: усі числа дають GPAW, PySCF, xTB і SevenNet, а модель готує вхідні файли, ставить розрахунок у чергу й читає звіт. Досвід цієї роботи показав і межу такого поділу. Мовна модель добре пише код і пояснює результат, але може впевнено повторити хибне число або підписати число одного методу під геометрією іншого. Тому кожне число, яке потрапляє в текст, проходить через скрипт звірки з первинним файлом, а не через пам’ять моделі. Саме з цієї вимоги й виріс аудитор.

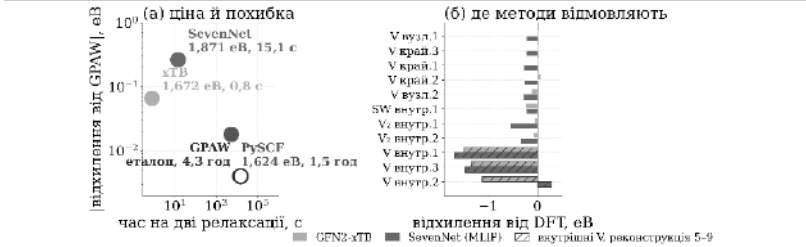


Рисунок 5. Чотири рівні опису, ціна проти точності: (а) одна задача, пара 5–7 коронену, час на дві повні релаксації на одному потоці проти відхилення від GPAW; (б) одинадцять конфігурацій [4]-триангулену, звірених із DFT, заштриховано внутрішні моновакансії з мотивом 5–9

6. Обговорення результатів

Головний практичний підсумок роботи в тому, що питання «потенціал чи DFT» перестає бути питанням про модель загалом і стає питанням про кожну конфігурацію окремо. Опублікована оцінка пом'якшення [11] дає одне число на модель. Тут показано, що для однієї й тієї самої моделі похибка змінюється майже на два порядки: від 0,013 еВ на повороті Стоуна–Уельса до 1,112 еВ на дивакансії з двома розірваними зв'язками. Отже, для скринінгу важливий не «середній» рівень довіри, а правило, яке для кожної структури каже, чим її рахувати. Для конвеєра скринінгу це означає простий поділ роботи. Конфігурації без розірваних зв'язків — повороти зв'язків та ізомери — рахує лише потенціал: похибка тут становить соті частки електронвольта (0,013 еВ для поворотів); так само точно відтворюється заміщення азотом (до 0,068 еВ). Абсолютні енергії заміщення потребують одного розрахунку DFT на елемент. Оскільки зсув сталий для елемента, одна пара чисел DFT і MLIP на будь-якій позиції калібрує всі інші позиції цього елемента. Конфігурації з розірваними зв'язками C–H потенціал використовує лише для впорядкування, а найкращих кандидатів передає на DFT. Для них можлива й поправка 0,2–0,4 еВ на зв'язок, але її нахил виміряно лише на коронені, тож для інших фрагментів вона потребує перевірки. Підрозділ 3.5 показує, що похибка не росте з розміром, і це дає підстави сподіватися на переносність поправки, але не доводить її. Виграш у часі визначає найдорожчий щабель: сто конфігурацій потенціалом — це менше як пів години, еталоном — понад два тижні. GFN2-xTB за 0,8 с придатний як перший фільтр для ізомерів і вакансій, але не для абсолютних енергій заміщення, де його середня похибка становить 1,419 еВ.

Межі цих висновків треба назвати прямо. По-перше, досліджено одну модель, SevenNet 7net-omni-i12, і дві її голови, які не лежать на одній шкалі й відтворюють різні рівні теорії (PBE і ωB97M-V). Чи повторюється нахил «еВ на розірваний зв'язок» в інших універсальних потенціалах, поки невідомо; якщо так, він є властивістю навчальних вибірок, а не окремої архітектури. По-друге, еталоном є DFT з функціоналом PBE, а не експеримент. Сам еталон має похибку: за даними DMC функціонал PBE занижує енергію заміщення вуглецю кремнієм у графені на 0,6–0,8 еВ (3,59–3,77 проти 4,4(1) еВ) [25]. Тому всі числа тут є похибками потенціалу відносно PBE, а не відносно істини. По-третє,

досліджено одну родину плоских фрагментів із насиченими воднем краями. Для функціоналізованих або неплоских фрагментів число розірваних зв'язків може виявитися не єдиною ознакою. По-четверте, випадок фосфору лишається нез'ясованим: потенціал міняє місцями крайову й вузлову позиції, і гіпотеза про вихід гетероатома з площини ще не перевірена.

7. Висновки та перспективи подальших досліджень

1. Пом'якшення універсального MLIP залежить від класу конфігурації. На 28 парних конфігураціях вакансій і дивакансій коронену потенціал занижує енергію утворення в кожному випадку. Поворот Стоуна–Уельса, який не розриває зв'язків, відтворюється з розходженням 0,013 еВ.

2. Заниження росте з числом розірваних зв'язків, і це число видно зі структури. Воно зростає від 0,299 еВ для вакансії з цілим краєм до 1,112 еВ для дивакансії з двома розірваними зв'язками C–H, тобто 0,2–0,4 еВ на зв'язок. Частина цієї енергії - спінова стабілізація до 0,372 еВ, якої в потенціалі немає. Похибка не росте з розміром фрагмента: на ряду $C_{13}H_9$–$C_{54}H_{18}$ вона в середньому становить 0,133 еВ.

3. Легування підтверджує критерій для відносних енергій. Для азоту розходження GPAW і MLIP не перевищує 0,068 еВ. Для B, O, S і Si зсув однаковий для всіх позицій елемента (розкид до 0,24 еВ), тобто його визначає резервуар, а не позиція. Виняток - фосфор. Конвеєр має порівнювати різниці між позиціями, а не абсолютні значення.

4. Енергію заміщення визначає глибина позиції, а не розмір точки. При однаковій відстані до краю розкид між $C_{16}H_{10}$, $C_{24}H_{12}$ і $C_{54}H_{18}$ не перевищує 0,36 еВ для N, O, P і Si. Для вакансій форма фрагмента важить більше за розмір, а енергія глибинної вакансії виходить на плато вже при C_{54}.

5. Там, де потенціал помиляється в абсолютних значеннях, він зберігає порядок: структури дефекту, розділені понад п'ятьма електронвольтами, розташовані так само, як у DFT, а 17 карт легування з 19 дають ту саму найвигіднішу позицію.

6. Розкид енергії всередині класу симетрії показує ненадійні позиції, але не доводить правильності. Так, хибні структури внутрішніх позицій C_{54} і C_{96} мали розкид лише 0,02–0,04 еВ. Структуру позиції треба перевіряти окремо від енергії.

7. Три прості правила й аудитор перевірок роблять потенціал придатним для конвеєра. Число розірваних зв'язків, розкид усередині класу симетрії та структура позиції обчислюються зі структури й не залежать від моделі. У ланцюжку xTB → MLIP → DFT попередній відбір триває секунди, а години розрахунків DFT витрачаються лише на відібраних кандидатів.

Перспективи подальших досліджень. Найближчий крок - з'ясувати випадок фосфору: перевірити, чи виходить гетероатом із площини і як це пов'язано з положенням сходинки в профілі вглиб. Далі планується співлегування парами B+N і перевірка критерію на інших універсальних потенціалах.

Подяки та використані інструменти

Під час підготовки статті використано велику мовну модель Claude Opus 5 (Anthropic) у середовищі Claude Code: нею написано скрипти розрахунків і

перевірок, побудовано рисунки з первинних файлів та відредаговано текст. Усі розрахункові результати отримано пакетами GPAW, PySCF, xTB і SevenNet; кожне число статті звірено з первинними файлами скриптом. Остаточні формулювання, висновки й відповідальність за них належать авторам.

Література

[1] Geng, Z., He, Z., Huang, Y., Li, Y., Zhong, X., Deng, W., Zou, G., Zhu, Y., Tian, L., Guo, M., Hou, H., & Ji, X. (2026). Recent advances on graphene quantum dots and their derivatives for energy storage devices. *International Journal of Extreme Manufacturing, 8*(2), Article 022005. https://doi.org/10.1088/2631-7990/ae2221

[2] El Haddad, Y., Ouarrad, H., & Drissi, L. B. (2024). Insights into the optoelectronic behaviour of heteroatom doped diamond-shaped graphene quantum dots. *RSC Advances, 14*(18), 12639–12649. https://doi.org/10.1039/d4ra00603h

[3] Kohn, W., & Sham, L. J. (1965). Self-consistent equations including exchange and correlation effects. *Physical Review, 140*(4A), A1133–A1138. https://doi.org/10.1103/PhysRev.140.A1133

[4] Tuzhykov, A., Kiv, A., Soloviev, V., Bielinskyi, A., Kavetskyy, T., Slusarenko, M., & Korotysh, V. (2025). Artificial intelligence methods in quantum chemistry. In P. Petkov, M. E. Achour, & C. Popov (Eds.), *Nanotechnological advances in environmental, cyber and CBRN security* (pp. 67–83). Springer. https://doi.org/10.1007/978-94-024-2316-7_4

[5] Behler, J., & Parrinello, M. (2007). Generalized neural-network representation of high-dimensional potential-energy surfaces. *Physical Review Letters, 98*(14), Article 146401. https://doi.org/10.1103/PhysRevLett.98.146401

[6] Bartók, A. P., Payne, M. C., Kondor, R., & Csányi, G. (2010). Gaussian approximation potentials: The accuracy of quantum mechanics, without the electrons. *Physical Review Letters, 104*(13), Article 136403. https://doi.org/10.1103/PhysRevLett.104.136403

[7] Batzner, S., Musaelian, A., Sun, L., Geiger, M., Mailoa, J. P., Kornbluth, M., Molinari, N., Smidt, T. E., & Kozinsky, B. (2022). E(3)-equivariant graph neural networks for data-efficient and accurate interatomic potentials. *Nature Communications, 13*, Article 2453. https://doi.org/10.1038/s41467-022-29939-5

[8] Batatia, I., Kovács, D. P., Simm, G. N. C., Ortner, C., & Csányi, G. (2022). MACE: Higher order equivariant message passing neural networks for fast and accurate force fields. *Advances in Neural Information Processing Systems, 35*, 11423–11436. https://proceedings.neurips.cc/paper_files/paper/2022/hash/4a36c3c51af11ed9f34615b81edb5bbc-Abstract-Conference.html

[9] Chen, C., & Ong, S. P. (2022). A universal graph deep learning interatomic potential for the periodic table. *Nature Computational Science, 2*(11), 718–728. https://doi.org/10.1038/s43588-022-00349-3

[10] Park, Y., Kim, J., Hwang, S., & Han, S. (2024). Scalable parallel algorithm for graph neural network interatomic potentials in molecular dynamics simulations. *Journal of Chemical Theory and Computation, 20*(11), 4857–4868. https://doi.org/10.1021/ acs.jctc.4c00190

[11] Deng, B., Choi, Y., Zhong, P., Riebesell, J., Anand, S., Li, Z., Jun, K., Persson, K. A., & Ceder, G. (2025). Systematic softening in universal machine learning interatomic potentials. *npj Computational Materials, 11*, Article 9. https://doi.org/10.1038/s41524-024-01500-6

[12] Koskinen, P., Malola, S., & Häkkinen, H. (2008). Self-passivating edge reconstructions of graphene. *Physical Review Letters, 101*(11), Article 115502. https://doi.org/10.1103/PhysRevLett.101.115502

[13] Rodrigues, J. N. B., Gonçalves, P. A. D., Rodrigues, N. F. G., Ribeiro, R. M., Lopes dos Santos, J. M. B., & Peres, N. M. R. (2011). Zigzag graphene nanoribbon edge reconstruction

with Stone–Wales defects. *Physical Review B, 84*(15), Article 155435. https://doi.org/10.1103/PhysRevB.84.155435

[14] Jiang, W., Liu, Z.-F., Wu, Q.-P., & Xiao, X. (2025). Role of edge reconfiguration in generating corner states in zigzag graphene nanoribbons. *Physica E: Low-Dimensional Systems and Nanostructures, 172*, Article 116260. https://doi.org/10.1016/ j.physe.2025.116260

[15] Kiv, A., Soloviev, V., Tuzhykov, A., Kavetskyy, T., Hoivanovych, N., Šauša, O., Rusnák, J., Švajdlenková, H., Ostrauskaite, J., Bielinskyi, A., & Slusarenko, M. (2025). Machine learning interatomic potentials and orientational defects in polymers. In P. Petkov, M. E. Achour, & C. Popov (Eds.), *Nanotechnological advances in environmental, cyber and CBRN security* (pp. 91–104). Springer. https://doi.org/10.1007/978-94-024-2316-7_6

[16] Tuzhykov, A., Soloviev, V., Kiv, A., & Bielinskyi, A. (2026). *Formation energies of point defects in pyrene: DFT against MLIP* [Manuscript submitted for publication]. South Ukrainian National Pedagogical University named after K. D. Ushynsky.

[17] Tuzhykov, A., Soloviev, V., Kiv, A., & Bielinskyi, A. (in press). Edge-scaling softening of a universal machine-learned potential: Point-defect formation energies in a coronene graphene quantum dot. In *Proceedings of the XIV International Scientific and Practical Conference "Information Control Systems and Technologies" (ICST-ODESA-2026), Odesa, Ukraine, September 22–24, 2026*. CEUR Workshop Proceedings.

[18] Enkovaara, J., Rostgaard, C., Mortensen, J. J., Chen, J., Dułak, M., Ferrighi, L., Gavnholt, J., Glinsvad, C., Haikola, V., Hansen, H. A., Kristoffersen, H. H., Kuisma, M., Larsen, A. H., Lehtovaara, L., Ljungberg, M., Lopez-Acevedo, O., Moses, P. G., Ojanen, J., Olsen, T., … Jacobsen, K. W. (2010). Electronic structure calculations with GPAW: A real-space implementation of the projector augmented-wave method. *Journal of Physics: Condensed Matter, 22*(25), Article 253202. https://doi.org/10.1088/0953-8984/22/25/253202

[19] Hjorth Larsen, A., Mortensen, J. J., Blomqvist, J., Castelli, I. E., Christensen, R., Dułak, M., Friis, J., Groves, M. N., Hammer, B., Hargus, C., Hermes, E. D., Jennings, P. C., Jensen, P. B., Kermode, J., Kitchin, J. R., Kolsbjerg, E. L., Kubal, J., Kaasbjerg, K., Lysgaard, S., … Jacobsen, K. W. (2017). The atomic simulation environment—A Python library for working with atoms. *Journal of Physics: Condensed Matter, 29*(27), Article 273002. https://doi.org/10.1088/1361-648X/aa680e

[20] Perdew, J. P., Burke, K., & Ernzerhof, M. (1996). Generalized gradient approximation made simple. *Physical Review Letters, 77*(18), 3865–3868. https://doi.org/10.1103/PhysRevLett.77.3865

[21] Kim, J., You, J., Park, Y., Lim, Y., Kang, Y., Kim, J., Jeon, H., Ju, S., Hong, D., Lee, S. Y., Choi, S., Kim, Y., Lee, J. W., & Han, S. (2026). Optimizing cross-domain transfer for universal machine learning interatomic potentials. *Nature Communications, 17*, Article 3432. https://doi.org/10.1038/s41467-026-70195-8

[22] Sun, Q., Zhang, X., Banerjee, S., Bao, P., Barbry, M., Blunt, N. S., Bogdanov, N. A., Booth, G. H., Chen, J., Cui, Z.-H., Eriksen, J. J., Gao, Y., Guo, S., Hermann, J., Hermes, M. R., Koh, K., Koval, P., Lehtola, S., Li, Z., … Chan, G. K.-L. (2020). Recent developments in the PySCF program package. *The Journal of Chemical Physics, 153*(2), Article 024109. https://doi.org/10.1063/5.0006074

[23] Weigend, F., & Ahlrichs, R. (2005). Balanced basis sets of split valence, triple zeta valence and quadruple zeta valence quality for H to Rn: Design and assessment of accuracy. *Physical Chemistry Chemical Physics, 7*(18), 3297–3305. https://doi.org/10.1039/b508541a

[24] Bannwarth, C., Ehlert, S., & Grimme, S. (2019). GFN2-xTB—An accurate and broadly parametrized self-consistent tight-binding quantum chemical method with multipole electrostatics and density-dependent dispersion contributions. *Journal of Chemical Theory and Computation, 15*(3), 1652–1671. https://doi.org/10.1021/acs.jctc.8b01176

[25] Thomas, D. M., Asiri, Y., & Drummond, N. D. (2022). Point defect formation energies in graphene from diffusion quantum Monte Carlo and density functional theory. *Physical Review B, 105*(18), Article 184114. https://doi.org/10.1103/PhysRevB.105.184114

[26] Lahouari, A., Rogal, J., & Tuckerman, M. E. (2026). Automated machine learning pipeline: Large language models-assisted automated data set generation for training machine-learned interatomic potentials. *Journal of Chemical Theory and Computation, 22*(1), 305–317. https://doi.org/10.1021/acs.jctc.5c01610

[27] Jacobs, R., Morgan, D., Attarian, S., Meng, J., Shen, C., Wu, Z., Xie, C. Y., Yang, J. H., Artrith, N., Blaiszik, B., Ceder, G., Choudhary, K., Csányi, G., Cubuk, E. D., Deng, B., Drautz, R., Fu, X., Godwin, J., Honavar, V., Wood, B. M. (2025). A practical guide to machine learning interatomic potentials – Status and future. *Current Opinion in Solid State and Materials Science, 35*, Article 101214. https://doi.org/ 10.1016/j.cossms. 2025.101214

ACCURACY LIMITS OF MACHINE-LEARNING POTENTIALS FOR DEFECTS AND DOPING OF GRAPHENE QUANTUM DOTS

Tuzhikov A.[1], Dr.Sci., Solovyov V.[1,3], Dr.Sci., Kiv A.[2], Belinsky A.[4]

[1]State Institution 'K. D. Ushynsky South Ukrainian National Pedagogical University', Ukraine,

[2]Ben-Gurion University of the Negev, Israel,
[3]Vadym Hetman Kyiv National Economic University, Ukraine,
[4]State University of Economics and Technology, Ukraine

Abstract. *Machine-learning interatomic potentials (MLIPs) increasingly replace density functional theory (DFT) for screening hundreds of structures, yet they systematically underestimate the energy of structures far from equilibrium. The origin of this deficit, and when such a model can be trusted, remain unclear. The purpose is to find a structural descriptor that controls the error of a universal MLIP. The universal potential SevenNet is compared with spin-polarised DFT (GPAW, PBE) for coronene $C_{24}H_{12}$: every structure is relaxed once, and both methods score the same geometry with the same formula. Across 28 vacancy and divacancy configurations the potential always underestimates the formation energy, from 0.299 eV for a vacancy with an intact edge to 1.112 eV for a divacancy with two broken C–H bonds, i.e. 0.2–0.4 eV per broken bond. The Stone–Wales rotation, which breaks no bonds, is reproduced to 0.013 eV. For nitrogen doping the deviation from DFT stays within 0.068 eV, while for B, O, S and Si the offset is the same for all sites of an element, i.e. it stems from the reservoir, not the site. The applicability of the potential is set by the number of broken bonds, not by model accuracy in general. Together with the energy spread within a symmetry class and a site-topology check, this gives three simple rules for an automated pipeline in which xTB → MLIP pre-screening takes seconds and hours-long DFT is reserved for selected candidates.*

Keywords: *graphene quantum dot, point defect, substitutional doping, density functional theory, surrogate model, machine-learning interatomic potential, SevenNet, systematic softening, model validation, coronene, agentic systems, formation energy.*

УДК 004.85:620.9
DOI

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ГЕТЕРОГЕННИХ ДАНИХ У СИСТЕМАХ ПРОАКТИВНОГО УПРАВЛІННЯ ЕНЕРГОСПОЖИВАННЯМ СМАРТ-ОБ'ЄКТІВ

Dr.Sci.,Арсірій О.[1][0000-0001-8130-9613] , Dr.Sci., Арсірій В.[2][0000-0003-3617-8487], Засідько А.[3][0000-0001-5197-0435], Крантовський І.[4][0009-0008-4801-2453]

[1,3,4]Національний університет «Одеська політехніка», Україна,
[2] Одеська державна академія будівництва та архітектури, Україна
EMAIL: [1]e.arsiriy@gmail.com, [2]vasyly.arsiriy@gmail.com,
[3]andzasidko@gmail.com, [4]illya20020814@gmail.com

Анотація. *Мета. Розробити модель енергетичного стану смарт-об'єкта та методи підготовки й класифікації гетерогенних даних для інформаційного забезпечення проактивного управління енергоспоживанням. Методи. Поєднано показники лічильників, погодні дані й метадані будівель; розглянуто статистичні ознаки ковзних вікон, нормалізацію та кластеризацію K-means. На стратифікованій вибірці обсягом 30 000 записів Building Data Genome 2 порівняно логістичну регресію, лінійний метод опорних векторів, гаусівський наївний байєсівський класифікатор, Soft Voting і Stacking. Цільові класи низького, середнього й високого споживання сформовано окремо для типів лічильників. Результати. Найкращі наведені показники отримано для Stacking: accuracy 0,6458, зважена F1-міра 0,6621 та AUC 0,8343. Для Soft Voting отримано accuracy 0,5937, зважену F1-міру 0,5837 та AUC 0,8023. Запропоновано зв'язок між класифікацією станів і цільовою функцією вартості енергії з урахуванням мережевих та експлуатаційних обмежень. Висновки. Класифікація створює інформаційну основу для подальшого вибору керуючих дій. Наведені результати характеризують розпізнавання класів споживання; економічний ефект, дотримання комфорту й точність прогнозу на заданому горизонті потребують окремої перевірки.*

Ключові слова:*гетерогенні дані, енергоспоживання будівель, проактивне управління, кібер-фізична система, кластеризація K-means, класифікація станів, ансамблеве навчання.*

Постановка проблеми

Управління енергоспоживанням будівель потребує узгодження роботи обладнання з доступною потужністю, ціною енергії та умовами експлуатації. Для України ця задача пов'язана також із відновленням енергетичної інфраструктури [1]. У лікарнях, освітніх закладах, офісах і житлових будівлях допустимість зміни навантаження визначають функції обладнання та потреби користувачів. Однакові показники лічильника можуть відповідати різним погодним умовам і режимам роботи, тому їх необхідно аналізувати разом із контекстом. Реагування на попит (Demand Response, DR) передбачає зміну споживання у відповідь на цінові або стимулювальні сигнали [2]. Проактивне управління енергоспоживанням (Proactive Energy Consumption Management, PECM) використовує оцінку стану об'єкта та очікувані зміни навантаження для підготовки рішення. Воно може застосовуватися в програмах DR. Його інформаційна основа потребує узгодженого представлення вимірювань і контексту.

Досліджуємо формалізацію стану смарт-об'єкта, підготовку гетерогенних даних і порівняння класифікаторів. Зв'язок із керуванням задаємо через цільову функцію витрат та обмеження.

Аналіз попередніх досліджень

Для аналізу енергоспоживання застосовують фізичні моделі, моделі, навчені за даними, та їх поєднання. Wei та співавтори узагальнюють підходи до прогнозування й класифікації споживання [3]. Вибір методу залежить від доступних вимірювань і задачі оцінювання; гетерогенність даних ускладнює підготовку ознак, але не виключає фізичного моделювання. Shaikh та співавтори розглядають управління енергетичними витратами й комфортом користувачів [4]. Огляд Mariano-Hernández та співавторів охоплює прогнозне керування, управління попитом, оптимізацію та діагностику несправностей [5]. Ці напрями пов'язують оцінювання стану будівлі з її експлуатаційними обмеженнями.

Albadi та El-Saadany систематизують програми DR на електроенергетичних ринках [6]; Charoen та співавтори описують реалізацію DR із системою енергоменеджменту будівлі [7]. DR охоплює різні способи керування, тому його не слід ототожнювати з реакцією лише після виникнення піку. Kathirgamanathan та співавтори аналізують кероване даними прогнозне управління для використання енергетичної гнучкості будівель [8]. Воно потребує узгодження прогнозу й моделі реакції обладнання. Afram і Janabi-Sharifi розглядають моделі систем опалення, вентиляції та кондиціювання [9], які забезпечують фізичне обґрунтування допустимих режимів. Amasyali та El-Gohary узагальнюють дослідження прогнозування енергоспоживання за даними [10], а Himeur та співавтори — аналітику даних у системах автоматизації будівель [11]. Різна частота, одиниці й повнота вимірювань зумовлюють потребу в узгодженому векторі ознак. Building Data Genome 2 (BDG2) поєднує вимірювання споживання, погоду й метадані будівель [12]. Divina та співавтори дослідили Stacking для короткострокового прогнозування електроспоживання [13]. Результати числового прогнозування не можна безпосередньо переносити на класифікацію режимів, тому ансамблі потребують порівняння в межах поставленої задачі. Мітка рівня споживання не визначає керуючої дії: вона не встановлює допустимості вимкнення обладнання чи дотримання комфорту. Ці умови потрібно задавати окремо.

Невирішені питання

У BDG2 немає готових міток, які визначали б режим або оптимальну стратегію управління. Потрібно узгодити вимірювання різних лічильників, представлення стану та цільові класи, обґрунтувати розмітку й порівняти моделі її розпізнавання.

Мета та завдання дослідження

Мета роботи - розробити модель енергетичного стану та методи інтелектуального аналізу гетерогенних даних для інформаційного забезпечення РЕСМ. Для цього формалізуємо стан смарт-об'єкта й відокремлюємо його класифікацію від вибору дії. Формуємо вектор ознак із показників лічильників, погодного й часового контексту та характеристик будівлі; розглядаємо попередню обробку, часові статистики та кластерну розмітку. Порівнюємо

логістичну регресію, лінійний SVM, гаусівський наївний байєсівський класифікатор, Soft Voting і Stacking; задаємо цільову функцію вартості енергії та обмеження управління. Експериментальна задача полягає в оцінюванні класифікації на BDG2. Перевірка економії та роботи замкненого контуру належить до подальших досліджень.

Модель енергетичного стану смарт-об'єкта

Смарт-об'єктом вважаємо будівлю або комплекс приміщень, вимірювання якого доступні для аналізу та підготовки керуючих дій. Їх допустимість залежить від призначення обладнання: перенесення допоміжної операції й зупинка критичного споживача мають різні наслідки. Показники лічильників характеризують споживання, контекст - умови його формування, метадані - відмінності між будівлями.

За цими даними класифікатор визначає режим; вибір дії додатково потребує оцінки її наслідків. Кібер-фізична система (Cyber-Physical System, CPS) поєднує обладнання, мережі й сенсори з інформаційними засобами аналізу та керування. Структуру смарт-об'єкта задає кортеж (1):

$$O = (P, C, A) \tag{1}$$

У (1) P є фізичною складовою, C - контекстом, A - множиною допустимих дій. Контекст містить погоду, календарний режим і додаткові параметри управління. Нехай x_i є вектором вимірювань і контексту на кроці i, а S_i - описом стану, сформованим із їх історії. Оператор виділення ознак Ф узагальнює вікно, яке закінчується на кроці і (2). Розмір w задає кількість відліків. Для погодинних даних w = 24 охоплює добу, а після добового агрегування - 24 доби. Розмірність S_i залежить від кількості змінних і статистик.

$$S_i = \Phi(x_{i-w+1,\dots,} x_i) \tag{2}$$

Набір статистик числової змінної подано в (3):

$$S_i = (\mu_w, \sigma_w, CV_w, trend_w, \max_w, \min_w) \tag{3}$$

Середнє μ характеризує рівень показника, σ - розкид, trend - його лінійну зміну; max і min зберігають діапазон значень. $CV = \sigma/\mu$ описує відносну мінливість невід'ємного показника споживання до центрування. За близького до нуля μ потрібне окреме правило обробки. CV не слід автоматично застосовувати до температури в градусах Цельсія або Z-нормалізованих ознак.

Поєднання кількох вікон описує швидкі зміни й тривалі цикли. Воно не гарантує стаціонарності: сезонність і зміни режимів можуть зберігатися. Представлення (1) – (3) використовуємо для класифікації рівнів споживання, яку відокремлюємо від оптимізації дій. Цільова множина Y = {Low, Medium, High} описує низький, середній і високий рівні для відповідного типу лічильника. Назви призначають після впорядкування центроїдів.

За ймовірнісних оцінок класифікатора $f(S_i; \theta)$ рішення задає (4):

$$\hat{y}_i = \arg\max_{y \in Y} p_\theta(y \mid S_i) \tag{4}$$

$p_\theta(y \mid S_i)$ є оцінкою класу y. Для прогнозу на горизонт h потрібні пари (S_i, y_{i+h}); розпізнавання y_i за S_i не є перевіркою такого прогнозу.

Навчання параметричної моделі узагальнює функція втрат із регуляризацією (5):

$$J_{cls}(\theta) = \frac{1}{n}\sum_{i=1}^{n} l(y_i, f(S_i;\theta)) + \lambda_{cls}\Omega(\theta) \quad (5)$$

де n - кількість навчальних прикладів, y_i - цільова мітка, ℓ - втрата, Ω - регуляризатор, λ_{cls} - його вага. Логістична регресія використовує логарифмічну втрату, SVM - іншу оптимізаційну постановку, а GaussianNB оцінює розподіли ознак.

Оптимальні параметри моделей із такою функцією визначає (6):

$$\theta^* = \arg\min_{\theta} J_{cls}(\theta) \quad (6)$$

Втрата класифікації відрізняється від витрат управління: практична ціна помилки залежить від обладнання, контексту й доступних дій. Високий рівень споживання в робочі години може бути допустимим, тоді як середній за зниженого ліміту потужності потребуватиме перегляду режиму. На рисунку 1 подано перетворення вимірювань і контексту на ознаки та класифікаційне рішення. Його зв'язок із керуванням задає завершальна ланка; експеримент перевіряє класифікаційну частину.

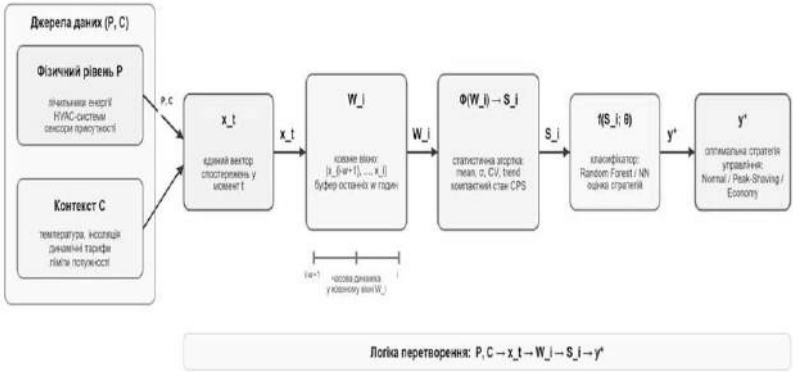


Рисунок 1. Структура проактивного управління енергоспоживанням смарт-об'єкта

Формування вектора ознак стану

Формування ознак охоплює вибір джерел, узгодження вимірювань, попередню обробку та опис динаміки. Кластеризація доповнює цей процес цільовими мітками. Відокремлюємо дані BDG2 від додаткових входів управління. BDG2 [12] містить дані 1 636 будівель і 3 053 лічильників на 19 майданчиках у Північній Америці та Європі. Погодинні ряди за 2016–2017 роки доповнено погодою й метаданими. Вісім типів лічильників охоплюють електроенергію, охолоджену воду, газ, гарячу воду, іригацію, сонячну генерацію, пару та воду.

Склад інформації для представлення стану наведено в таблиці 1. BDG2 не містить повного опису допустимих дій, обладнання та вимог комфорту. Різні типи лічильників мають різні шкали; їх показники не можна безпосередньо додавати. Фізичний баланс потребує узгоджених одиниць, а розмітка рівнів - урахування типу показника. Метадані описують характеристики й призначення будівель.

Таблиця 1

Вимірювання та контекстні змінні для представлення стану смарт-об'єкта

Категорія	Приклади змінних	Походження та обмеження
Показники лічильників	Електроенергія, газ, вода, пара; гаряча й охолоджена вода; іригація, сонячна генерація	BDG2; одиниці й наявність визначаються типом лічильника. Добові суми не є миттєвою потужністю.
Погода	Температура, вітер, тиск, опади	Погодні файли BDG2; узгодження за майданчиком і часом.
Метадані	Тип використання будівлі, площа, доступні характеристики	Метадані BDG2; не всі поля заповнені для всіх будівель.
Календар	Часова мітка, день тижня, сезон	Формуються за часом; робочий розклад і свята потребують додаткових відомостей.
Параметри управління	Тариф за одиницю енергії, ліміт потужності, вимоги комфорту	Додаткові входи PECM; не є штатними полями BDG2 та не підтверджують економічного ефекту експерименту.

Перенесення моделі на інший об'єкт потребує окремої перевірки. Після агрегування до добових сум втрачається внутрішньодобова інформація. Такі записи дозволяють класифікувати добові рівні, але не визначають погодинного перевищення потужності. Вимірювання BDG2 характеризують реальні будівлі; реакція обладнання на керуючу дію в цьому наборі не перевіряється.

З урахуванням таблиці 1 вектор спостереження має вигляд (7):

$$x_i = (p_i, c_{ext,i}, c_{time,i}, c_{econ,i}, b), \tag{7}$$

де p_i - доступні показники лічильників; $c_{ext,i}$ - погода, $c_{time,i}$ - календар, $c_{econ,i}$ - економічні параметри, b - метадані. Тариф і ліміт потужності є додатковими входами PECM, а не штатними полями BDG2.

Попередня обробка узгоджує пропуски, аномалії, часові мітки, масштаби та категоріальні ознаки за однаковими правилами. Високий показник не слід автоматично вилучати як викид: він може бути реальним піком. Для пропусків можливе заповнення, але прогнозна задача допускає тільки дані, відомі на момент рішення. Дані синхронізують за будівлею, майданчиком і часом. Енергію за інтервали підсумовують, погодні показники зазвичай усереднюють; ураховують частоту й часовий пояс. Погоду отримують із файлів BDG2, календарні ознаки - з часових міток. Робочий розклад, свята, тариф і мережевий ліміт потребують додаткових відомостей.

Масштабування числових ознак за Z-оцінкою визначає (8):

$$z_{i,j} = \frac{x_{i,j} - \mu_j}{\sigma_j} \tag{8}$$

де μ_j і σ_j - параметри j-ї ознаки, визначені за навчальними даними. Сталу ознаку з $\sigma_j = 0$ обробляють окремо; до тестових даних застосовують уже оцінені параметри.

Нормалізація зменшує вплив масштабів, але не гарантує однакового впливу ознак на модель. Номінальні категорії кодують окремими індикаторами (one-hot encoding), а для циклічного часу можливе кодування періодичності.

Числовий код не повинен створювати штучний порядок категорій. Параметри обробки зберігають разом із моделлю для застосування до нових спостережень. Ковзне вікно містить тільки дані до кроку і включно. Його узгодження з моментом прогнозу потрібне для часової перевірки [14]. Вікно з w відліків задає (9):

$$W_i = (x_{i-w+1}, ..., x_i) \tag{9}$$

Вектори x_τ у (9) мають структуру (7); використовуються лише доступні на відповідний момент параметри. Якщо цільовою міткою є y_{i+h}, дані після і не включають до S_i. Оператор Ф перетворює вікно на статистичні ознаки (3). Для погодинних даних короткі вікна 3–6 годин описують швидкі зміни, а 24–168 годин - добові й тижневі цикли. Для добових записів потрібна інша сітка. Розміри добирають на навчальних та валідаційних даних. Чіткість кластерів може допомагати добору ознак, але не доводить якості прогнозування або управління. Оскільки BDG2 не має готових класів споживання, розмітку формують кластеризацією. K-means групує близькі спостереження; K-means++ задає спосіб ініціалізації центроїдів [15]. У загальному методі групують вектори ознак, а в експерименті - логарифмічно перетворені показники окремо за типами лічильників. Критерій K-means наведено в (10), де z_i є представленням для кластеризації:

$$J_{clust} = \sum_{k=1}^{K} \sum_{z_i \in C_k} \| z_i - \mu_k \|^2 \tag{10}$$

де C_k - кластер, μ_k - його центроїд. В одновимірному випадку їх упорядковують і називають Low, Medium, High. Центроїд не встановлює нормативного або оптимального режиму.

K = 3 відповідає прийнятій інтерпретації рівнів. У загальному методі кількість кластерів можна досліджувати за зміною внутрішньокластерної суми квадратів. Мітки використовують як цільову змінну класифікатора.

Класифікація станів і постановка задачі управління

Після розмітки порівнюємо базові моделі й ансамблі. Цільова функція управління задає спосіб подальшого використання їхніх відповідей. Для прогнозної задачі тестові періоди повинні наставати після навчальних [14]. Масштабування, добір параметрів, розмітку та балансування узгоджують із поділом. Наведений експеримент використовує випадковий поділ і оцінює розпізнавання класів. Логістична регресія й SVM перевіряють лінійні межі, GaussianNB - умовні розподіли ознак. Soft Voting усереднює їхні ймовірності; Stacking навчає модель другого рівня. Для дії a ∈ Адоп вартість енергії та штраф за перевищення потужності задає (11):

$$J_{cost}(a) = \sum_{\tau=1}^{H} c_\tau \hat{E}_\tau(a) + \lambda_{net} \sum_{\tau=1}^{H} [\max(0, \hat{P}_\tau(a) - P_{\max,\tau})]^2 \tag{11}$$

де $\hat{E}_\tau(a)$ - оцінка енергії після дії, c_τ - тариф, $\hat{P}_\tau(a)$ - оцінка потужності, $P_{max,\tau}$ - ліміт, λ_{net} - вага штрафу, H - горизонт планування. Для інших енергоносіїв потрібні власні одиниці й тарифи.

Адоп враховує технічні межі, обов'язкові операції та комфорт. Якщо ліміт потужності є жорсткою вимогою, його задають явним обмеженням; самого

штрафу недостатньо. Без моделі наслідків дії та перевірки допустимості мітка класу не визначає оптимальної стратегії. Функція (11) є постановкою задачі, для якої передбачено подальшу реалізацію.

Експериментальна перевірка на даних BDG2

Порівняння виконано на вибірці BDG2 обсягом 30 000 записів. Підготовка охоплює добове агрегування, додавання контексту, обробку ознак, розмітку, балансування та навчання п'яти моделей. Файли вимірювань перетворено з широкого формату в довгий: запис містить будівлю, тип лічильника, час і показник. Погодинні вимірювання агреговано до добових сум; добовий запис є одиницею класифікації. Приєднано майданчик, тип використання, площу та інші доступні метадані будівель. Температуру, вітер, тиск і опади приєднано за майданчиком та часом і агреговано до добового рівня. Вибірку стратифіковано за типами лічильників із random_state = 42. Пропуски заповнено медіанами, категорії перетворено one-hot кодуванням, числові ознаки масштабовано StandardScaler. Ці перетворення виконано до поділу вибірки. Для кожної пари «будівля - тип лічильника» обчислено групові середнє та стандартне відхилення за доступною вибіркою. Багатомасштабні вікна й додаткові статистики (3) належать до загального методу. Для кожного типу лічильника застосовано $\log(1 + q)$, де q - невід'ємний добовий показник, та K-means із трьома кластерами. Центроїди впорядковано й названо Low, Medium, High. Гістограми наведено на рисунку 2, спільне представлення — на рисунку 3.

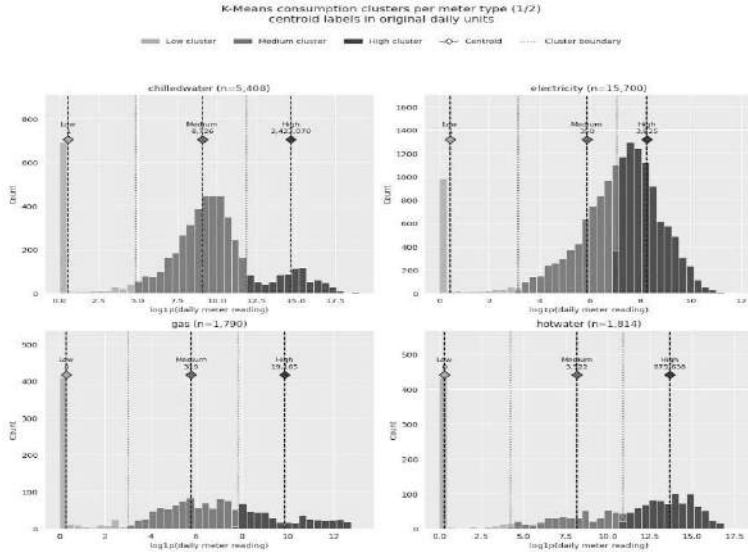


Рисунок 2а. Розподіли log(1 + q) і центроїди кластерів для охолодженої води, електроенергії, газу та гарячої води

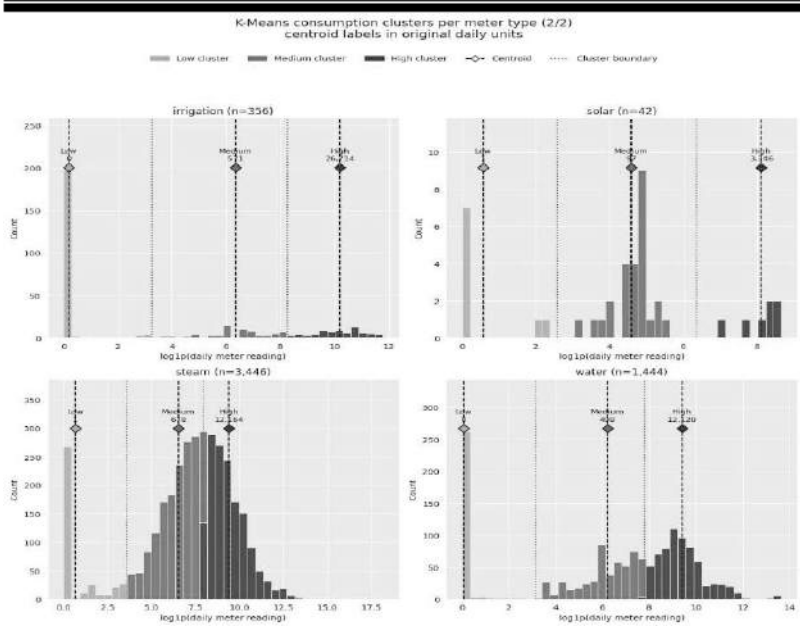


Рисунок 2б. Розподіли log(1 + q) і центроїди кластерів для іригації, сонячної генерації, пари та води

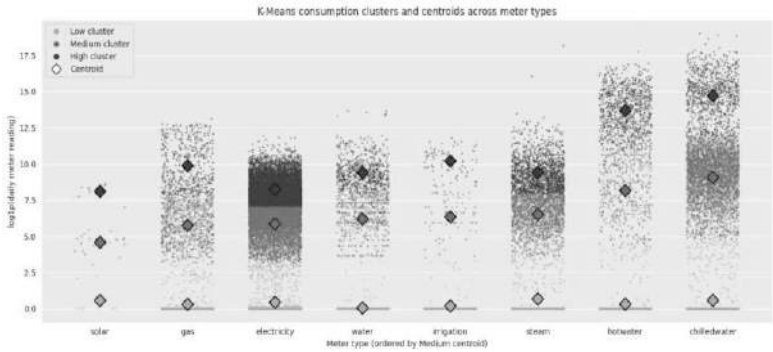


Рисунок 3. Розподіли добових показників і центроїди K-means у логарифмічній шкалі за типами лічильників

Підписи центроїдів отримано зворотним перетворенням із логарифмічної шкали; це не арифметичні середні вихідних показників. Класи різних типів лічильників не задають однакової кількості енергії. Розподіл за класами показано на рисунку 4. Поточний показник q вилучено з ознак класифікатора. Застосовано випадковий стратифікований за класом поділ 80/20 із random_state = 42. Навчальну частину збалансовано SMOTE [16] шляхом інтерполяції між сусідами міноритарного класу; тестову частину не балансували. Порівняно

логістичну регресію з регуляризацією, лінійний SVM із калібруванням ймовірностей, GaussianNB, Soft Voting та Stacking із логістичною метамоделлю.

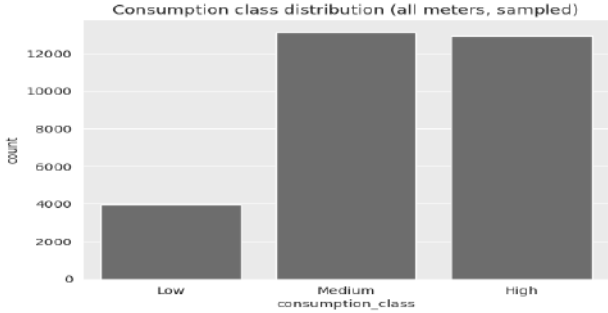


Рисунок 4. Кількість записів вибірки за класами Low, Medium і High

Логістична регресія. Логістична функція переводить лінійний предиктор у ймовірність бінарного класу [17]. Peng та співавтори розглядають опис і подання результатів цієї моделі [18]. Для трьох класів потрібне багатокласове правило. Мультиноміальна модель використовує softmax (12):

$$p_k(S) = \frac{\exp(\eta_k)}{\sum_{i=1}^{K}\exp(\eta_i)} \tag{12}$$

$\eta_k = \beta_{0k} + \beta_k^T S$ є предиктором класу k, β_{0k} - зміщенням, β_k - коефіцієнтами. Сума ймовірностей дорівнює одиниці; рішення приймають за (4). Можливий також підхід «один проти решти». Коефіцієнти оцінюють із регуляризацією. У дослідженні гіперпараметри добирали рандомізованим пошуком із перехресною валідацією.

Наївний байєсівський класифікатор припускає умовну незалежність ознак за заданого класу [19]. У нашій задачі ознаки описують будівлю, погоду й вимірювання, а клас - рівень споживання. Апостеріорну ймовірність задає (13):

$$p(k \mid S) = \frac{p(S \mid k)\pi_k}{p(S)} \tag{13}$$

де π_k - апріорна ймовірність класу, $p(S|k)$ - правдоподібність, $p(S)$ - нормувальна величина. Незалежність дає (14). Тут d - кількість ознак.

$$p(S \mid k) = \prod_{j=1}^{d} p(S_j \mid k) \tag{14}$$

Для GaussianNB числову ознаку за класом моделюють нормальним розподілом (15) [20]:

$$p(S_j \mid k) = \frac{1}{\sqrt{2\pi\sigma_{jk}^2}}\exp(-(S_j - \mu_{jk})^2 / (2\sigma_{jk}^2)) \tag{15}$$

μ_{jk} і σ^2_{jk} оцінюють для ознаки j та класу k. Кореляція між ознаками й відмінності від нормального розподілу можуть обмежувати придатність цієї моделі.

Метод опорних векторів будує межу між класами з урахуванням зазору й допустимих порушень [21]. У дослідженні використано лінійний SVM; багатокласове рішення поєднує двокласові підзадачі.

Для лінійного SVM межу задає $v^T S + b = 0$, де v - ваги, b - зміщення. Позначення v відокремлюємо від розміру вікна w.

Для пар (S_i, t_i), $t_i \in \{-1; +1\}$, постановку з м'яким зазором задає (16):

$$\min_{v,b,\xi}\left(\frac{1}{2}\| v \|^2 + C_{svm}\sum_{i=1}^{n}\xi_i\right) \tag{16}$$

за обмежень (17):

$$t_i(v^T S_i + b) \geq 1 - \xi_i, \xi_i \geq 0, i = 1,...,n \tag{17}$$

C_{svm} визначає вагу порушень, ξ_i - їх допустиму величину. Ймовірнісні оцінки для ансамблів отримують додатковим калібруванням SVM. Лінійне ядро обчислює скалярний добуток векторів ознак. У наведеному експерименті інші ядра не порівнювалися.

Soft Voting усереднює ймовірності трьох базових моделей за (18). Правила поєднання класифікаторів розглянуто Kittler та співавторами [22]. Якість відповіді залежить від оцінок кожного компонента.

$$p_{vote,k}(S) = \frac{1}{3}\sum_{m=1}^{3} p_{m,k}(S) \tag{18}$$

Stacking навчає метамодель на відповідях базових моделей [23]; рішення узагальнює (19). Для навчання другого рівня використовують прогнози на прикладах, відокремлених від навчання відповідної базової моделі. У дослідженні метамоделлю є логістична регресія.

$$\hat{y}_{stack} = g(p_1(S), p_2(S), p_3(S)) \tag{19}$$

Оцінювання. Accuracy розраховано для всієї тестової частини; precision, recall, F1 та AUC - зі зважуванням за числом прикладів класу. AUC використовує «один проти решти», specificity - макроусереднення. M_{kl} позначає кількість записів справжнього класу k, віднесених до l; n_k - підтримку класу, N — загальне число записів. Площу під ROC-кривою класу k визначає (20):

$$AUC_k = \int_0^1 TPR_k(u)du, u = FPR_k \tag{20}$$

$TPR_k = TP_k/(TP_k + FN_k)$; $FPR_k = FP_k/(FP_k + TN_k) = 1 - \text{specificity}_k$. Для зваженої AUC покласові значення усереднюють із вагами n_k/N.

Accuracy визначає діагональ матриці помилок (21):

$$Accuracy = \frac{\sum_{k=1}^{K} M_{kk}}{N} \tag{21}$$

TP_k, TN_k, FP_k і FN_k обчислюють для класу k проти решти. Для загальної accuracy використовують (21), уникаючи повторного рахування записів.

Покласову F1-міру задає (22):

$$F1_k = \frac{2\,\mathrm{Pr}ecision_k\,\mathrm{Re}call_k}{\mathrm{Pr}ecision_k + \mathrm{Re}call_k} \tag{22}$$

Precision_k визначає частку правильних відповідей серед передбачених записів класу k (23):

$$\Pr ecision_k = \frac{TP_k}{TP_k + FP_k} \tag{23}$$

Зважені precision і F1 отримують усередненням покласових величин із вагами n_k/N. R_{ecall_k} є часткою знайдених записів справжнього класу k (24):

$$\mathrm{Re}\, call_k = \frac{TP_k}{TP_k + FN_k} \tag{24}$$

За однозначної багатокласової класифікації зважена recall дорівнює accuracy. Для нульового знаменника потрібно задавати окреме правило.

Багатокласовий MCC визначає (25) [24]:

$$MCC = \frac{cs - \sum_{k=1}^{K} p_k \cdot t_k}{\sqrt{(s^2 - \sum_{k=1}^{K} p_k^2)(s^2 - \sum_{k=1}^{K} t_k^2)}}, \tag{25}$$

$c = \Sigma_k M_{kk}$, $s = N$, $p_k = \Sigma_l M_{lk}$ - передбачена підтримка класу, $t_k = \Sigma_l M_{kl}$ - справжня. MCC враховує всі елементи матриці. Специфічність класу k задає (26):

$$Specificity_k = \frac{TN_k}{TN_k + FP_k} \tag{26}$$

У таблиці 2 specificity є середнім за K класами. Багатокласову логарифмічну втрату визначає (27):

$$LogLoss = -\frac{1}{N}\sum_{i=1}^{N}\sum_{k=1}^{K} y_{ik} \log(p_{ik}), \tag{27}$$

де y_{ik} - індикатор справжнього класу, p_{ik} - його ймовірність. Для числового обчислення нульові ймовірності обмежують малим додатним значенням.

Менша LogLoss є кращою. Числові результати п'яти моделей наведено в таблиці 2.

Таблиця 2

Метрики класифікації рівнів добового споживання

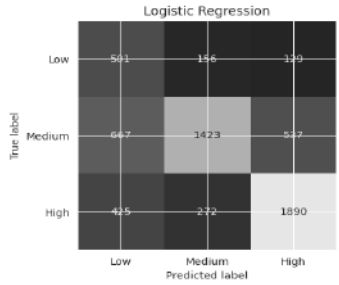
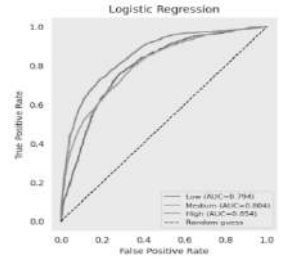
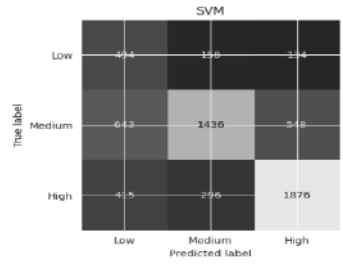
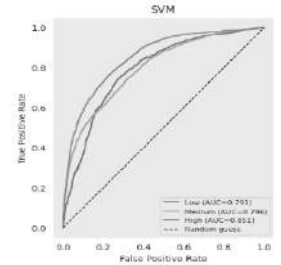
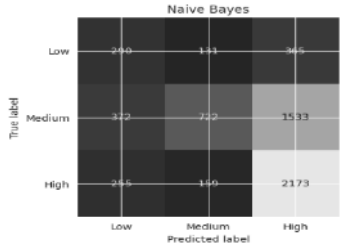
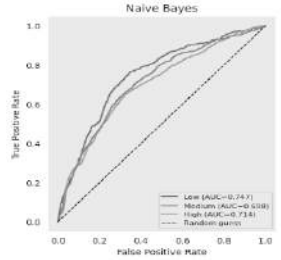
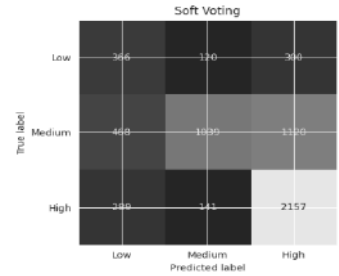
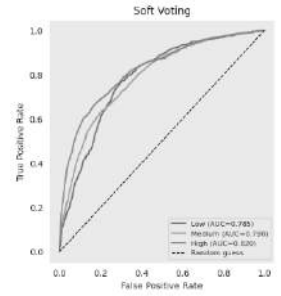
Метрика	Логістична регресія	Лінійний SVM	GaussianNB	Soft Voting	Stacking
Accuracy	0.6357	0.6343	0.5308	0.5937	0.6458
Precision	0.6966	0.6906	0.5839	0.6526	0.706
Recall	0.6357	0.6343	0.5308	0.5937	0.6458
F1 Score	0.6503	0.6482	0.4998	0.5837	0.6621
AUC	0.8242	0.8194	0.7112	0.8023	0.8343
LogLoss	0.7997	0.8052	4.8586	0.8577	0.7792
MCC	0.4488	0.4436	0.2658	0.3723	0.464
Specificity	0.8228	0.8209	0.7459	0.7871	0.8287

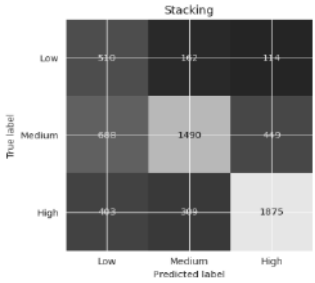
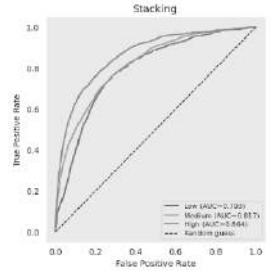
У таблиці 3 наведено матриці помилок і покласові ROC-криві. Матриця показує напрям помилок за обраного рішення, а ROC-крива — ранжування при різних порогах. За наведеними метриками Stacking має accuracy 0,6458, зважену F1-міру 0,6621 та AUC 0,8343. Для Soft Voting відповідні значення становлять 0,5937, 0,5837 та 0,8023. Повний набір числових результатів подано в таблиці 2. F1-міри логістичної регресії та лінійного SVM становлять 0,6503 і 0,6482. Для GaussianNB отримано F1 0,4998 та LogLoss 4,8586. Матриці помилок і покласові ROC-криві наведено в таблиці 3. Експериментальне порівняння

стосується класифікації рівнів добового споживання. Оптимізаційний модуль (11) задає наступну частину системи, для якої потрібна окрема реалізація.

Таблиця 3

Матриці помилок і покласові ROC-криві базових та ансамблевих класифікаторів

Модель	Матриця помилок	ROC-криві
Логістична регресія		
Лінійний SVM		
GaussianNB		
Soft Voting		

Модель	Матриця помилок	ROC-криві
Stacking		

Висновки та перспективи подальших досліджень

Розроблено інформаційну модель стану смарт-об'єкта, що поєднує вимірювання, контекст і допустимі дії. Класифікацію споживання відокремлено від вибору дії, для якого потрібна оцінка її наслідків. Метод формування ознак охоплює узгодження джерел, попередню обробку та опис часових вікон. Тарифи, мережеві ліміти й вимоги комфорту є додатковими входами управління. Кластеризація логарифмічно перетворених добових показників окремо за типами лічильників сформувала Low, Medium і High. Ці мітки використовуються для порівняння класифікаторів. На 30 000 записах із випадковим поділом 80/20 порівняно п'ять моделей. Для Stacking отримано accuracy 0,6458, F1 0,6621, AUC 0,8343 та LogLoss 0,7792. Метрики наведено в таблиці 2, матриці помилок і ROC-криві - у таблиці 3. Цільова функція поєднує вартість енергії та штраф за перевищення потужності; допустимі дії визначають технічні й експлуатаційні обмеження. Оптимізатор потребує подальшої реалізації. Подальші дослідження мають визначити горизонт прогнозу, перевірити моделі за часовим поділом і оцінити їх перенесення між будівлями. Після реалізації управління необхідно порівняти його з базовим режимом за вартістю енергії, перевищенням потужності та дотриманням комфорту. Це дасть підставу для кількісної оцінки ефекту РЕСМ.

Використання генеративних інструментів

Під час підготовки тексту використано Gemini 3.1 Flash-Lite та Gemini 3.1 Pro для мовного редагування й перекладу. Для цієї редакції застосовано Codex (GPT-6.1 Sol та GPT-6 Luna) для допомоги в редагуванні, перевірці бібліографії та технічній підготовці документа. Відповідальність за аргументацію, достовірність результатів і остаточне формулювання висновків належить авторам.

Література

[1] Tröndle, T., Melnyk, O., Tutova, O., Porieva, V., Neumann, F., Staffell, I., & Patt, A. (2024). Rebuilding Ukraine's energy supply in a secure, economic, and decarbonised way. *Environmental Research: Infrastructure and Sustainability, 4*(3), 031002. https://doi.org/10.1088/2634-4505/ad6738

[2] Palensky, P., & Dietrich, D. (2011). Demand side management: Demand response, intelligent energy systems, and smart loads. *IEEE Transactions on Industrial Informatics, 7*(3), 381–388. https://doi.org/10.1109/TII.2011.2158841

[3] Wei, Y., Zhang, X., Shi, Y., Xia, L., Pan, S., Wu, J., Han, M., & Zhao, X. (2018). A review of data-driven approaches for prediction and classification of building energy consumption. *Renewable and Sustainable Energy Reviews, 82*, 1027–1047. https://doi.org/10.1016/j.rser.2017.09.108

[4] Shaikh, P. H., Nor, N. B. M., Nallagownden, P., Elamvazuthi, I., & Ibrahim, T. (2014). A review on optimized control systems for building energy and comfort management of smart sustainable buildings. *Renewable and Sustainable Energy Reviews, 34*, 409–429. https://doi.org/10.1016/j.rser.2014.03.027

[5] Mariano-Hernández, D., Hernández-Callejo, L., Zorita-Lamadrid, A., Duque-Pérez, O., & Santos García, F. (2021). A review of strategies for building energy management system: Model predictive control, demand side management, optimization, and fault detect & diagnosis. *Journal of Building Engineering, 33*, 101692. https://doi.org/10.1016/j.jobe.2020.101692

[6] Albadi, M. H., & El-Saadany, E. F. (2008). A summary of demand response in electricity markets. *Electric Power Systems Research, 78*(11), 1989–1996. https://doi.org/10.1016/j.epsr.2008.04.002

[7] Charoen, P., Kitbutrawat, N., & Kudtongngam, J. (2022). A demand response implementation with building energy management system. *Energies, 15*(3), 1220. https://doi.org/10.3390/en15031220

[8] Kathirgamanathan, A., De Rosa, M., Mangina, E., & Finn, D. P. (2021). Data-driven predictive control for unlocking building energy flexibility: A review. *Renewable and Sustainable Energy Reviews, 135*, 110120. https://doi.org/10.1016/j.rser.2020.110120

[9] Afram, A., & Janabi-Sharifi, F. (2014). Review of modeling methods for HVAC systems. *Applied Thermal Engineering, 67*(1–2), 507–519. https://doi.org/10.1016/j.applthermaleng.2014.03.055

[10] Amasyali, K., & El-Gohary, N. M. (2018). A review of data-driven building energy consumption prediction studies. *Renewable and Sustainable Energy Reviews, 81*, 1192–1205. https://doi.org/10.1016/j.rser.2017.04.095

[11] Himeur, Y., Elnour, M., Fadli, F., Meskin, N., Petri, I., Rezgui, Y., Bensaali, F., & Amira, A. (2023). AI-big data analytics for building automation and management systems: A survey, actual challenges and future perspectives. *Artificial Intelligence Review, 56*(6), 4929–5021. https://doi.org/10.1007/s10462-022-10286-2

[12] Miller, C., Kathirgamanathan, A., Picchetti, B., Arjunan, P., Park, J. Y., Nagy, Z., Raftery, P., Hobson, B. W., Shi, Z., & Meggers, F. (2020). The Building Data Genome Project 2, energy meter data from the ASHRAE Great Energy Predictor III competition. *Scientific Data, 7*(1), 368. https://doi.org/10.1038/s41597-020-00712-x

[13] Divina, F., Gilson, A., Goméz-Vela, F., García Torres, M., & Torres, J. F. (2018). Stacking ensemble learning for short-term electricity consumption forecasting. *Energies, 11*(4), 949. https://doi.org/10.3390/en11040949

[14] Hyndman, R. J., & Athanasopoulos, G. (2021). *Forecasting: Principles and practice* (3rd ed.). OTexts. https://otexts.com/fpp3/

[15] Arthur, D., & Vassilvitskii, S. (2007). k-means++: The advantages of careful seeding. In H. Gabow (Ed.), *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms* (pp. 1027–1035). Society for Industrial and Applied Mathematics. https://research.google/pubs/k-means-the-advantages-of-careful-seeding/

[16] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research, 16*, 321–357. https://doi.org/10.1613/jair.953

[17] Cox, D. R. (1958). The regression analysis of binary sequences. *Journal of the Royal Statistical Society: Series B (Methodological), 20*(2), 215–232. https://doi.org/10.1111/j.2517-6161.1958.tb00292.x

[18] Peng, C.-Y. J., Lee, K. L., & Ingersoll, G. M. (2002). An introduction to logistic regression analysis and reporting. *The Journal of Educational Research, 96*(1), 3–14. https://doi.org/10.1080/00220670209598786

[19] Rish, I. (2001). An empirical study of the naive Bayes classifier. In *Proceedings of the IJCAI-01 Workshop on Empirical Methods in Artificial Intelligence* (pp. 41–46). https://faculty.cc.gatech.edu/~isbell/reading/papers/Rish.pdf

[20] John, G. H., & Langley, P. (1995). Estimating continuous distributions in Bayesian classifiers. In P. Besnard & S. Hanks (Eds.), *Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence* (pp. 338–345). Morgan Kaufmann Publishers. https://arxiv.org/abs/1302.4964

[21] Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning, 20*(3), 273–297. https://doi.org/10.1007/BF00994018

[22] Kittler, J., Hatef, M., Duin, R. P. W., & Matas, J. (1998). On combining classifiers. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 20*(3), 226–239. https://doi.org/10.1109/34.667881

[23] Wolpert, D. H. (1992). Stacked generalization. *Neural Networks, 5*(2), 241–259. https://doi.org/10.1016/S0893-6080(05)80023-1

[24] Gorodkin, J. (2004). Comparing two K-category assignments by a K-category correlation coefficient. *Computational Biology and Chemistry, 28*(5–6), 367–374. https://doi.org/10.1016/j.compbiolchem.2004.09.006

INTELLIGENT ANALYSIS OF HETEROGENEOUS DATA IN PROACTIVE ENERGY MANAGEMENT SYSTEMS OF SMART OBJECTS

Dr.Sci., Арсірій О.[1], Dr.Sci., Арсірій В.[2], Засідько А.[1], Крантовський І.[1]

[1] Odessa Polytechnic National University, Ukraine,
[2] Odessa State Academy of Civil Engineering and Architecture, Ukraine

Abstract. *Objective. To develop an energy-state model and methods for preparing and classifying heterogeneous data to support proactive energy consumption management in smart facilities. Methods. Meter readings, weather data and building metadata were combined. The methodological framework considers sliding-window statistics, normalization and K-means clustering. Logistic regression, linear support vector machines, Gaussian naive Bayes, Soft Voting and Stacking were compared using a stratified sample of 30,000 Building Data Genome 2 records. Low, Medium and High consumption classes were defined separately for each meter type. Results. Stacking achieved the best reported scores: accuracy of 0.6458, weighted F1 of 0.6621 and AUC of 0.8343. For Soft Voting, accuracy was 0.5937, weighted F1 was 0.5837 and AUC was 0.8023. A cost objective and operational constraints were formulated to connect state classification with subsequent control decisions. Conclusions. Classification provides an information basis for selecting control actions. The reported results concern recognition of consumption classes. Economic benefits, comfort compliance and prediction accuracy at a specified future horizon require separate evaluation.*

Keywords: *heterogeneous data, building energy consumption, proactive control, cyber-physical system, K-means clustering, state classification, ensemble learning.*

Section 2 Control, robotics, and distributed systems

UDC 004.5+681.5
DOI

MODELS OF HYBRID HUMAN-MACHINE CONTROL FOR ROBOTIC SYSTEMS

Ph.D., Yarmilko A.[1][0000-0003-2062-2694], **Marchenko S.**[2][0000-0003-1655-3091]
Bohdan Khmelnytsky National University of Cherkasy, Ukraine
EMAIL: [1]a-ja@ukr.net, [2]sv.marchenko1989@gmail.com

Abstract. *This paper presents a structured multimodal mission-oriented model of hybrid control for robotic systems operating under incomplete information, varying channel quality, real-time constraints, and operator involvement. Unlike conventional command or policy blending, shared control is organized through admissible event routing among operator, autonomous, mission, and safety handlers. The multimodal state comprises navigation, visual, communication, operator, system-computational, and energy channels. The model was evaluated using synthetic data in a discrete-time simulation of a declaratively specified multi-stage mission. The results demonstrated context-dependent channel relevance, correct mission and fallback transitions, rejection of conflicting operator initiative, and stable delegation among manual, shared, autonomous, and safety-oriented modes.*

Keywords. *Hybrid control; robotic systems; mission graph; shared autonomy; event routing; multimodal fusion; effective reactivity; operator initiative; safety fallback*

1. Problem Statement

The need for structural and system-level optimization of mission-oriented robotic systems has increased attention to synergy and deeper information cooperation between the human operator and the robotic machine [1]. This also applies to unmanned platforms intended for various purposes. At the current stage, progress in human-machine systems is expected within the hybrid intelligence paradigm [1, 2]. According to the concept of hybrid intelligence [2], a human-machine system should rationally combine human and machine capabilities while preserving the leading role of the human within the system. Under traditional control approaches based on maximizing control over system parameters, the amount of information processed by the human operator generally exceeds physiologically feasible levels. However, the tasks involved in executing an unmanned mission generally cannot be resolved by prioritizing the intellectual independence (autonomy) of the unmanned platform above all else. Accordingly, the optimal role of the human operator in a hybrid unmanned-mission control system is to compensate for limitations in the software that supports the platform's intelligent functions. The unmanned device itself should minimize the operator's physical, psychological, and emotional overload while current real-time control tasks are being solved. However, remote control of unmanned systems, particularly in complex and emotionally demanding applications, has a pronounced adverse effect on operators' mental health and performance [3, 4]. This necessitates an additional objective analysis of the phenomenon in the context of ensuring control-loop stability.

In this context, investigating mission control of a robotic system under variable channel quality, incomplete information, real-time constraints, and operator

participation is an important research task. Addressing it requires a mathematical model of multimodal hybrid control that combines performance, reactivity, mission execution, operator cognitive state, communication stability, and safety compliance within a single formalized system.

2. Analysis of Previous Studies

2.1 Hybrid Control, Shared Autonomy, and Human-Robot Teaming

Hybrid control of robotic systems is developing at the intersection of classical control theory, human-robot interaction, shared autonomy, mixed-initiative control, and runtime supervision. Human-robot interaction research emphasizes that robotic autonomy should be regarded as a variable allocation of functions among the human, the automatic controller, and the autonomous planner [5]. This conclusion is consistent with the concept of levels of automation, in which the human operator can act as a source of goals, supervisor, arbiter, or active executor depending on risk, task complexity, and information availability [6]. Recent reviews of practical human-robot teaming additionally emphasize three interrelated aspects of interaction: action coordination, communication, and cognitive compatibility [7]. For mission control, this triad has direct mathematical significance because each aspect becomes a separate observation channel and a constraint on the admissibility of a control decision. One of the basic mathematical approaches is action or policy blending, in which the resulting command is computed as a weighted combination of operator control and an autonomous proposal [8, 9]. This scheme is straightforward to interpret and performs well for tasks with a relatively stable goal; however, its sensitivity to intention-recognition errors creates a need for probabilistic models of the user's state. Model-free shared-autonomy and reinforcement-learning approaches reduce the number of a priori assumptions about the intention model, but shift the complexity to data, reward design, and safety validation [10]; in open-environment robotic systems, however, the value of this trade-off remains context-dependent. A separate line of research develops autonomy-infused teleoperation and perceptive shared autonomy, in which the autonomous system not only blends commands but also augments the operator's action with knowledge of the map, risk zones, the expected trajectory, uncertainty in the perception model, and the available local-planning modes [11]. Mathematical methods of hybrid control can also be systematized according to how control authority is coordinated. Compensatory methods use weighted sums, utility functions, Bayesian belief updates, soft penalties, MPC, or learning-based value functions. They are suitable for situations in which degradation of one channel can be partially compensated for by high confidence in another. Non-compensatory methods use thresholds, guard conditions, lexicographic ordering, minimax/Chebyshev criteria, control barrier functions, or safety filters. They are justified for constraints for which averaging would be conceptually inadmissible, such as collision risk, geofence violation, critical energy, a missed hard deadline, or loss of the command link during a takeover-critical phase. A mission-executing hybrid system therefore requires a composition of compensatory and non-compensatory rules associated with the mission phase and event class.

2.2 Mission-Oriented Specification and Semantic Mission Execution

The mission-oriented approach in robotics aims to separate high-level objectives from low-level motion commands. Current research on mission specification shows

that robotic systems employ state machines, behavior trees, hierarchical task networks, temporal logic, BPMN-like descriptions, DSLs, and task-oriented mission languages [12]. Comparative analyses of formalisms for robotic missions emphasize the absence of a single standard that supports goal hierarchy, reactivity, integration with humans and external devices, and runtime reconfiguration equally well.

Mission Specification Patterns for mobile robots describe recurring task patterns such as reach, patrol, avoid, visit, coverage, surveillance, search, return, and monitor [13]. They demonstrate that a formal mission specification should separate the routing task from the search or coverage task. Flight or motion from point A to point B performs a transit function, whereas a search phase requires specification of the search area, a coverage metric, visual or sensory conditions for candidate detection, a target-confirmation threshold, and rules for repeated inspection. Accordingly, the search stage should be represented as a semantic phase with its own state variables. Mathematically, mission-oriented control is most often implemented using state graphs, hybrid automata, timed automata, temporal logic, HTNs, or behavior trees. For hybrid control, the key requirement is the ability to preserve an unambiguous relationship between mission semantics and the admissible control mode. A mission graph with guard conditions, dynamic deadlines, coverage variables, and fallback transitions therefore provides a practical compromise.

2.3 Multimodal perception, channel reliability, and missing modalities

Multimodal modeling of robotic systems is based on the assumption that no single channel completely represents the system state. Reviews of multi-sensor fusion for autonomous systems distinguish sensor-level, feature-level, and decision-level fusion, emphasizing the trade-off among raw-data volume, feature informativeness, processing latency, and computational cost [14]. In robot vision, multimodality encompasses not only the conventional combination of cameras and sensors but also semantic scene understanding, VLM/LLM-assisted reasoning, navigation, localization, and domain adaptation [15]. Filtering methods such as the Kalman filter, extended/unscented Kalman filters, and sequential Monte Carlo remain fundamental for navigation-state estimation because they provide recursive estimates in the presence of a dynamics model and noisy measurements [16, 17]. The operator channel requires separate analysis because it includes a latent cognitive state. Psychophysiological measurements such as HRV, EDA, EEG, gaze, PERCLOS, response time, and task performance are widely used to estimate workload and fatigue [18]. For real-world control, missing modalities must also be considered: physiological sensors may be unavailable, invalid, or unacceptable for organizational reasons. The operator state in the model should therefore include not only an availability estimate but also a modality mask and observation uncertainty [19].

2.4 Reactivity, Real-Time Event Processing, and Energy-Aware Execution

Reactivity in embedded and cyber-physical systems is associated with processing events within temporal constraints. Classical real-time scheduling theory provides the basis for analyzing periodic and sporadic tasks using fixed-priority scheduling, rate-monotonic scheduling, and earliest-deadline-first scheduling [20, 21]. Weakly-hard real-time models describe streams in which a bounded number of missed deadlines is compatible with acceptable control quality [22]. Such models are particularly appropriate for video frames, informational telemetry, and auxiliary updates, whereas

hard safety events should retain a separate non-compensatory status [23]. In real-time robotic systems, reactivity encompasses queueing, event service, dispatching, network latency, feature processing, decision making, mission transitions, and command execution. Experimental studies of mission computers for robotic platforms show that energy-saving modes reduce consumption but introduce wake-up delays and alter the available reactivity budget [24]. Accordingly, the energy channel should be included in the model as a factor that affects inference, the system tick, event processing, and admissible control modes.

2.5 Safety Assurance, Runtime Guards, and Mission-Valid Delegation

Safety assurance for autonomous systems is currently being developed through control barrier functions, safety filters, reachability analysis, runtime assurance, and fallback supervision. Safety filters provide a unified intervention scheme in which a proposed control action is checked against a safe set and either projected onto or replaced by an admissible action [25]. Control barrier functions formalize invariance of the safe region and enable control synthesis under state/input constraints, disturbances, and sampled-data effects [26]. The runtime-assurance approach adds an architectural layer in which an advanced or learning-based controller may operate only within a monitored safety envelope; when the corresponding condition is violated, the system switches to a verified fallback controller [27]. For mission-oriented hybrid control, these methods have a dual role. They impose hard constraints on physical safety and also constrain delegation. If an operator command or autonomous recommendation violates the safety envelope, delegation must be rejected regardless of trust, expected utility, or mission benefit. If the operator channel degrades, the system may preserve the operator in the loop at the informational level, but it should not assign the operator hard real-time functions that require guaranteed response. Thus, a generalized model should combine safety filters, real-time reactivity, and human-autonomy teaming within a common mathematical requirement.

3. Unresolved Issues

The preceding analysis indicates the need for a consistent mathematical model that combines mission semantics, event-driven reactivity, multimodal channel evidence, operator initiative, safety constraints, and a delegation policy. It should support the investigation of the key research questions (RQ):

RQ1: How should the multimodal state of a robotic system be represented for mission-oriented hybrid control under varying information-channel quality, incomplete observations, and data uncertainty?

RQ2: How can the mission graph, current-phase semantics, sub-mission execution progress, and fallback decisions be connected within a unified mission-execution logic?

RQ3: How should the reactive suitability of a hybrid control system be evaluated with regard to temporal constraints, events of different criticality, and safety requirements?

RQ4: How should operator initiative be incorporated into mission-oriented hybrid control with regard to operator state, communication quality, mission validity, and safety?

RQ5: How can stable delegation among manual, shared, autonomous, and safety-oriented modes be ensured under channel degradation and mixed conflicting scenarios?

RQ5: як забезпечити стабільне делегування між ручним, спільним, автономним і safety-орієнтованим режимами за деградації каналів і змішаних конфліктних сценаріїв?

4. Objective of the Article

The objective of this article is to construct and perform scenario-based validation of a mathematical model for multimodal mission-oriented hybrid control of a robotic system. The model should connect event-level reactivity, channel estimates, semantic state, the mission graph, safety constraints, operator initiative, and the delegation policy into a sequential system of mappings, thereby enabling its configurations to be assessed according to the admissibility criteria for unmanned-mission control modes. The experiments are intended to assess the model's basic functional consistency and its sensitivity to isolated and compound degradations rather than to estimate the performance of a particular robotic platform.

5. A Multimodal Mission-Oriented Model of Hybrid Control

5.1. General Composition of a Model

The proposed model defines mission-oriented hybrid control as an ordered composition of policies that transforms heterogeneous events, channel observations, and operator actions into a mission-admissible control mode. The policy sequence fixes the causal order of information transformation from the primary event to the selection of an admissible control mode. A discrete time instant is denoted by $t_k = k\Delta t$, where $k \in N_0$ is the step number and Δt is the dispatcher-step duration. At step k, the model receives the set of raw events ε_k, asynchronous channel observations Y_k, the current mission state M_k, and, when present, operator initiative I_k^{op}. The complete computational chain is given in (1).

$$(E_k, Y_k, M_k, I_k^{op}) \to P_{sig}(F_k, \mu_k^{sig}) \to P_{feat} Z_k^0 \to \Phi_X(J_k^{cand}, X_k, \Omega_k) \to P_{fus} A_k \to P_{mis} \quad (1)$$

where P_{sig} is the signal-level policy; F_k is the set of validated event facts; μ_k^{sig} is the vector of aggregated signal metrics; P_{feat} is the feature-level policy; Z_k^0 is the set of base channel evidence; the superscript 0 indicates that the evidence is evaluated against the reference channel requirement before a specific mission transition is selected; Φ_X is the semantic interpreter; J_k^{cand} is the set of transitions whose structural triggers are satisfied; X_k s the collection of semantic vectors for these transitions; Ω_k is the collection of physical and temporal contexts; P_{fus} is the situational fusion policy; A_k is the set of candidate-transition estimates; P_{mis} is the

mission policy; D_k^{mis} is the mission decision; P_{del} is the delegation and event-routing policy; and D_k^{del} is the final mode decision.

The base sets of the model are defined in (2).

$$\begin{aligned} C &= \{nav, vis, comm, op, sys, eng\}, \\ Q &= \{HUMAN, SHARED1, SHARED2, SHARED3, AUTO, SAFE\}, \\ V &= \{transit, search, confirm, track, return, landing, landed\}, \end{aligned} \tag{2}$$

where C is the set of information and resource channels: navigation, visual, communication, operator, system-computational, and energy; Q is the set of event-processing and routing modes; and V is the set of mission-graph phases. The notations *SHARED1*, *SHARED2*,, and *SHARED3*, define different tables of terminal handlers for event classes.

The policy interfaces are formally defined by the mappings in (3).

$$\begin{aligned} &P_{sig} : E_k \times \Lambda_k^{sig} \to F_k \times \mu_k^{sig}, P_{feat} : Y_k \times \mu_k^{sig} \times \Theta_{cal} \to Z_k^0, \\ &\Phi_X : M_k \times F_k \times Z_k^0 \times O_k^{mis} \to J_k^{cand} \times X_k \times \Omega_k, \\ &P_{fus} : X_k \times \Theta_{fus} \to A_k, P_{mis} : M_k \times A_k \times \Omega_k \times R^{mis} \to D_k^{mis}, \\ &P_{del} : D_k^{mis} \times F_k \times X_k \times A_k \times I_k^{op} \times R^{del} \to D_k^{del}, \end{aligned} \tag{3}$$

where Λ_k^{sig} is the current load of the signal dispatcher; Θ_{cal} denotes the identified parameters of the channel models; O_k^{mis} contains direct mission measurements, including the completed route fraction, coverage, target posterior, duration of valid tracking, and distance to base; Θ_{fus} denotes parameters of calibrated fusion metamodels; R^{mis} denotes declarative mission requirements; and R^{del} denotes the reliability, timeliness, and safety requirements for the modes. The symbol R in R^{mis} and R^{del} denotes a set of requirements and is unrelated to R_{eff}.

The current mission state and direct mission measurements are defined in (4).

$$\begin{aligned} &M_k = \left\langle v_k, \tau_k^v, p_{path,k}, p_{\mathrm{cov},k}, p_{conf,k}, p_{track,k}, p_{ret,k}, p_k^{mis}, \varsigma_k, status_k \right\rangle, \\ &O_k^{mis} = \left\langle \hat{p}_{path,k}, \hat{p}_{\mathrm{cov},k}, \hat{p}_{conf,k}, \hat{p}_{track,k}, \hat{p}_{ret,k}, \hat{p}_k^{mis}, \right. \\ &\left. D_{route,k}^{rem}, D_{energy,k}^{rem}, D_{hazard,k}, D_{phase,k}^{rem}, d_{\mathrm{home},k} \right. \end{aligned} \tag{4}$$

where $v_k \in V$ is the active phase; τ_k^v is the time spent in that phase; $p_{path,k}$, $p_{\mathrm{cov},k}$, $p_{conf,k}$, $p_{track,k}$ and $p_{ret,k}$ are accumulated within-phase indicators;

p_k^{mis} is overall progress; ς_k is mission strain; and $status_k$ is the textual status. The hatted quantities in O_k^{mis} are direct measurements from the current step, from which p_{mis} updates the accumulated state M_{k+1}; they are not produced by the channel-estimation models.

The operator initiative used in (1) has the structure defined in (5).

$$I_k^{op} = \left\langle type_k^{init}, j_k^{init}, q_k^{init}, e_k^{init}, t_k^{init}, ctx_k^{hmi} \right\rangle, \tag{5}$$

where $type_k^{init}$ is the request type; j_k^{init} is the proposed transition or $\varnothing$; q_k^{init} is the requested mode; e_k^{init} is the initiative-carrying event; t_k^{init} is time; and ctx_k^{hmi} is the HMI context. The initiative is considered only after D_k^{mis} has been formed.

To eliminate data ambiguity between policies, four composite structures defined in (6) are used.

$$\begin{aligned} Z_k^{c,0} &= \left\langle s_k^{c,0}, a_k^c, u_k^{c,0} \right\rangle, \\ X_k(j) &= \left\langle x_k(j), h_k(j), n_k(j), r_k(j), e_k(j) \right\rangle, \\ A_k(j) &= \left\langle \sum_k (j), U_k(j), C_k^{conf}(j), L_j, C_j, A_k^{crit}(j), G_k^{hard}(j) \right\rangle, \\ D_k^{mis} &= \left\langle M_{k+1}, J_k^{cand}, J_k^{act}, J_k^*, D_k^{mis}(j_k^*), F_k^{mis}, A_k(j_k^*) \right\rangle, \end{aligned} \tag{6}$$

where $s_k^{c,0}$ is the base probability that the channel requirement is satisfied; a_k^c denotes data availability and freshness; $u_k^{c,0}$ is the standard uncertainty of the available support; x_k, h_k, n_k, r_k and e_k are, respectively, the spatial-visual, operator, communication, system-computational, and energy semantic components of transition $\sum_k (j)$ is the calibrated probability of transition success; $U_k(j)$ is its standard uncertainty; C_k^{conf} is diagnostic conflict; L_j is the list of relevant semantic components; C_j is the list of physical channels from which they originate; $A_k^{crit}(j)$ is the minimum support among the components declared critical; G_k^{hard} is the non-compensatory admissibility condition; J_k^{act} is the set of transitions with an open guard; J_k^* is the selected transition; and F_k^{mis} is the fallback transition or $\varnothing$.

The context $\Omega_k(j)$ is separated from the probabilistic vector $X_k(j)$ by (7).

$$\Omega_k(j)=\left\langle \xi_k, d_k^{safe}, T_{pipe,k}^{95}, D_{phase,k}^{rem}, D_{route,k}^{rem}, D_{energy,k}^{rem}, D_{hazard,k}, m_k^E(j), G_k^{sig,H} \right\rangle \quad (7)$$

Vector $\xi_k=\left\langle lat_k, lon_k, o_k^{risk}, w_k^{op}, T_k^{op}, T_k^{lat}, T_k^{jit}, p_k^{loss}, B_k, U_k^{cpu}, T_k^{\inf}, F_k^{fps} \right\rangle$ contains raw physical and operational quantities retained for context and traceability but not treated as additional fusion components. Here, lat_k and lon_k are coordinates; o_k^{risk} is the obstacle-risk estimate; w_k^{op} and T_k^{op} are operator workload and response time; T_k^{lat}, T_k^{jit}, p_k^{loss} and B_k are communication latency, jitter, loss ratio, and bandwidth; U_k^{cpu} is computational load; and $T_k^{\inf}$ and F_k^{fps} are inference latency and effective frame rate. d_k^{safe} is the margin to the safety-envelope boundary; $T_{pipe,k}^{95}$ is the 95th percentile of the system-pipeline time; $D_{phase,k}^{rem}, D_{route,k}^{rem}, D_{energy,k}^{rem}$ and $D_{hazard,k}$ are residual temporal budgets; $m_k^E(j)$ is the energy reserve; and $G_k^{sig,H}$ is the result of the signal-level hard check. Components $\Omega_k(j)$ are used as physical constraints in P_{mis} and P_{del}.

Raw quantities have a source index or physical unit and are introduced only into $\varepsilon_k, Y_k, O_k^{miss}$ or I_k^{op}. The superscript 0 is used only for base evidence $Z_k^{c,0}$ that has not yet been bound to a transition. After Φ_X, all probabilistic quantities must have transition index j. After P_{fus}, they are stored within $A_k(j)$. Symbol D denotes a time budget or deadline; T denotes realized or predicted time; p or s denotes probability; u or U denotes standard uncertainty and G denotes a binary non-compensatory condition.

5.2. Signal-Level Policy

The signal-level policy P_{sig} is the first policy in the chain (1). It performs the primary organization of events arriving from sensors, communication channels, the HMI, the planner, watchdog mechanisms, system timers, and the safety monitor.

An event $e_{k,i} \in E_k$ is represented by the tuple:

$$e_{k,i}=\left\langle id_i, src_i, c_i, cl_i, fam_i, sem_i, t_i^{arr}, T_i^{srv}, D_i, payload_i \right\rangle \quad (8)$$

In (8), i is the event sequence number at the current step; id_i is the unique identifier; src_i is the source; $c_i \in C$ is the channel; $cl_i \in \{hard, mission, soft, \text{info}\}$ is the temporal class; fam_i is the ontology family; sem_i is the functional semantics; t_i^{arr} is the arrival time; T_i^{srv} is the primary service time; D_i is the deadline measured

from arrival; and $payload_i$ is the minimum data payload required by subsequent handlers. The class and family are distinct attributes: the former determines temporal guarantees, whereas the latter determines the functional route.

For each event, a validated fact is formed:

$$f_{k,i} = \left\langle e_{k,i}, T_{k,i}^{queue}, T_{k,i}^{sig}, b_{k,i}^{miss}, b_{k,i}^{drop}, H_{k,i}^{hint} \right\rangle, \quad T_{k,i}^{sig} = T_{k,i}^{queue} + T_{k,i}^{srv} + T_{k,i}^{disp}. \tag{9}$$

Here, $T_{k,i}^{queue}$ is the queueing time; $T_{k,i}^{disp}$ is the dispatching overhead; $T_{k,i}^{sig}$ is the total signal-processing time; $b_{k,i}^{miss} = I \mid T_{k,i}^{sig} > D_i \mid$ is the deadline-miss indicator; $b_{k,i}^{drop}$ is the indicator of dropping due to overflow; and $H_{k,i}^{hint}$ is the preliminary routing hint. For hard events, $H_{k,i}^{hint} = H_{safe}$; operator events are directed to H_{op}; mission events are directed to H_{mis}; and all remaining events are passed to H_{feat}. The final handler is determined only in P_{del} after the control mode has been selected. The set $F_k = \{f_{k,i}\}$ is passed to Φ_X to determine transition triggers and to P_{del} for final routing of each event. The vector μ_k^{sig} is passed to P_{feat}; its component R_k^{sig} enters only the system-computational channel model as a descriptor of the input-stream state, whereas $G_k^{sig,H}$ is later transferred to the context $\Omega_k(j)$ and the hard gate. No other policy recomputes these quantities.

5.3. Feature-Level Policy

The feature-level policy transforms validated events and asynchronous measurements into channel evidence suitable for comparison within the active mission transition. According to (1) and (3), P_{feat} receives asynchronous observations $Y_k = \{Y_k^c : c \in C\}$ and signal metrics μ_k^{sig} from Section 5.2. Its output is the base evidence $Z_k^{c,0}$ for the reference channel requirement; adaptation of this evidence to a specific transition is performed only by Φ_X.

The probabilistic representation is used because the physical channel indicators have different units of measurement. Their common event is satisfaction of the transition requirement; therefore, the state of each channel is interpreted as the conditional probability of successfully satisfying that requirement. Each channel model predicts a binary success event on a calibration sample. Thus, the values $s_k^{c,0}$ share the same semantics – the estimated probability of satisfying the base channel requirement – while retaining their provenance in the corresponding physical channel.

For channel $c \in C$, where $C = \{nav.vis, comm, op, sys.eng\}$, the evidence is formed as

$$Z_k^{c,0} = \left\langle s_k^{c,0}, a_k^c, u_k^{c,0} \right\rangle, \chi_k^{c,0} = s_k^{c,0}, a_k^c \quad (10)$$

Here, the superscript 0 denotes the base requirement that has not yet been bound to a transition; $s_k^{c,0} \in [0,1]$ is the estimated probability of satisfying it; $a_k^c \in [0,1]$ is the probability that the data are available and current; $u_k^{c,0}$ is the standard uncertainty of the available support; and $\chi_k^{c,0}$ is the available base channel support. The symbols *nav*, *vis*, *comm*, *op*, *sys*, and *eng* denote the navigation, visual, communication, operator, system-computational, and energy channels, respectively.

For each $c \in C$, there is exactly one object $Z_k^{c,0}$. It stores the base probability, availability, standard uncertainty, and metadata of the physical features. The complete set $Z_k^0 = \{Z_k^{c,0}\}$ is passed directly to Φ_X.

5.4. Semantic Interpretation

The semantic interpreter Φ_X receives the current state M_k, validated facts F_k from Section 5.2, base evidence Z_k^0 from Section 5.3, and direct mission measurements O_k^{mis}. At this level, the transition index j is introduced for the first time: the same base evidence may have different semantic suitability for a telemetry update, an HMI confirmation, or a safety command. The candidate set is determined solely by the graph structure and the observed triggers:

$$J_k^{cand} = \{ j \in T : src(j) = v_k \wedge trig_j(M_k, F_k, O_k^{mis}) = 1 \} \quad (11)$$

Here, T is the set of graph transitions; v_k is the current phase in M_k; $src(j)$ is the source phase of the transition; and $trig_j$ is the declarative trigger predicate.

For each $j \in J_k^{cand}$, the semantic interpreter forms the vector

$$x_k(j) = \left\langle x_k(j), h_k(j), n_k(j), r_k(j), e_k(j) \right\rangle. \quad (12)$$

Here, $x_k(j)$ is spatial-visual support; $h_k(j)$ is operator-branch support; $n_k(j)$ is communication support; $r_k(j)$ is system-computational support; and $e_k(j)$ is energy support. The physical context (7) is formed in parallel. For each $j \in J_k^{cand}$, the policy returns the pair $\left\langle X_k(j), \Omega_k(j) \right\rangle$. The collection X_k is passed to P_{fus}; J_k^{cand} and $\Omega_k(j)$ are passed to P_{mis}; relevant $X_k(j)$ values are also subsequently used by P_{del} to evaluate event routes.

5.5. Global Situational Aggregation Policy

The global situational aggregation policy P_{fus} produces, for each candidate mission transition $j \in J_k^{cand}$, an aggregate situational estimate $\sum_k(j) \in [0,1]$ representing the degree of situational support for that transition. A high value indicates consistent support from the relevant components of the semantic state, whereas a low value indicates that the current situation is poorly suited to executing the transition. For the network component, the deadline associated with the transition class is used:

$$D_j^{comm} \in \{D_{safe}, D_{cmd}, D_{tlm}, D_{hmi}\}. \tag{13}$$

If the transition is associated with a safety message, D_{safe} is used; for control commands, D_{cmd}; for telemetry exchange, D_{tlm}; and for operator confirmation, D_{hmi}. A transition receives high support when all relevant semantic components $z_{i,k}(j)$ have high values. Degradation of a single relevant component reduces the overall situational estimate, which is consistent with supervisory-control logic: a physically admissible transition must also have sufficient reactive, energy, network, or operator support according to its type.

The situational estimate of mission transition *for the nominal mode* is defined by:

$$\begin{gathered}\sum_k(j) = m_k(j) \cdot \{A_k^{safe}(j)\}, \quad E_k^{crit} = 1, A_k^{cons}(j), \\ U_k(j) > \theta_U \vee C_k^{conflict}(j) > \theta_C A_k^{comp}(j),\end{gathered} \tag{14}$$

where θ_U is the global uncertainty threshold; $A_k^{safe}, A_k^{cons}, A_k^{comp}$ are the operators for compensatory, non-compensatory, and conservative transition logic, respectively; $C_k^{conflict}$ is the channel-conflict estimate; and θ_C is the channel-conflict threshold. The resulting estimate is passed to the mission policy P_{mis}, where it is used to rank candidate transitions, assess the admissibility of the active transition, select a fallback branch, and form the data required by the delegation policy P_{del}.

5.6. Mission Policy

The mission policy P_{mis} receives M_k, the candidate set J_k^{cand}, and contexts $\Omega_k(j)$ from Φ_X, as well as the estimates $A_k(j)$ from P_{fus}. Accordingly, P_{mis} only compares the predicted success with the physical budgets and declarative requirements of the graph. The policy output has the structure:

$$D_k^{mis} = \left\langle M_{k+1}, J_k^{cand}, J_k^{act}, j_k^*, D_k^{mis}(j_k^*), F_k^{mis}, A_k(j_k^*) \right\rangle. \tag{15}$$

Here, $J_k^{act} = \{j \in J_k^{cand} : g_k(j) = 1\}$; F_k^{mis} is the fallback transition, which is formed only when no nominal admissible transition exists or when an explicit fallback

condition is satisfied. The field $A_k(j_k^*)$ is passed to P_{del} without repeated fusion. For each transition, the source, target phase, criticality class, priority, base horizon, fallback, and list of relevant components are specified declaratively. Priority is a scenario requirement used only to resolve conflicts among simultaneously admissible transitions with the same reliability level.

5.7. Delegation Policy

The delegation policy P_{del} receives the completed mission decision D_k^{mis}, validated events F_k, the semantic vector $X_k(j_k^*)$, the situational estimate $A_k(j_k^*)$, and operator initiative I_k^{op}. It does not re-estimate the channels, modify $\sum_k$, or open mission guard conditions. Its task is to compare modes according to the success of routing precisely those events that are relevant to the already selected transition. The result has the form:

$$D_k^{del} = \left\langle q_k, q_k^{raw}, Q_k^{adm}, Q_k^R, \mathrm{R}_{\mathrm{e}\,ff,k}(q_k, j_k^*), R_k^{evt}, d_k^{init}, d_k^{fb} \right\rangle. \quad (16)$$

Here, q_k is the mode after switching-stability verification; q_k^{raw} is the statistically best candidate before the residence-time check; Q_k^{adm} is the set of physically admissible modes; Q_k^R is the set of modes whose lower reactivity bound satisfies the transition requirement; R_k^{evt} is the final event-routing table; $d_k^{init} \in \{accept, defer, override, none\}$ is the initiative decision; and d_k^{fb} is the fallback decision. The HUMAN, SHARED1, SHARED2, SHARED3, AUTO, and SAFE modes define rules for routing event classes to the operator, mission, autonomous, or safety handler. For transition j, the set of structurally admissible modes $Q_k^{str}(j)$ is determined by the presence of human and autonomous components in its specification.

6. Experimental Configuration and Scenario Matrix

The experimental configuration is built around an external mission description. The graph topology, geometric goals, temporal constraints, priorities, guards, and fallback states are specified in JSON markup (Figure 1). The hybrid-control policies receive the active state and candidate transitions. Hybrid management policies receive an active state and candidate transitions after loading and structural validation. The configuration contains 14 states and 23 explicitly declared transitions. The main route covers the preflight check, takeoff, flight to the search area, search, target tracking, return, landing, and the terminal LANDED state. Route Replanning, Search Repositioning, and Target Reacquisition form local adaptation branches. Compact Telemetry is a separate communication-adaptation state. Safe Loiter and Aborted implement the safety branch of this configuration.

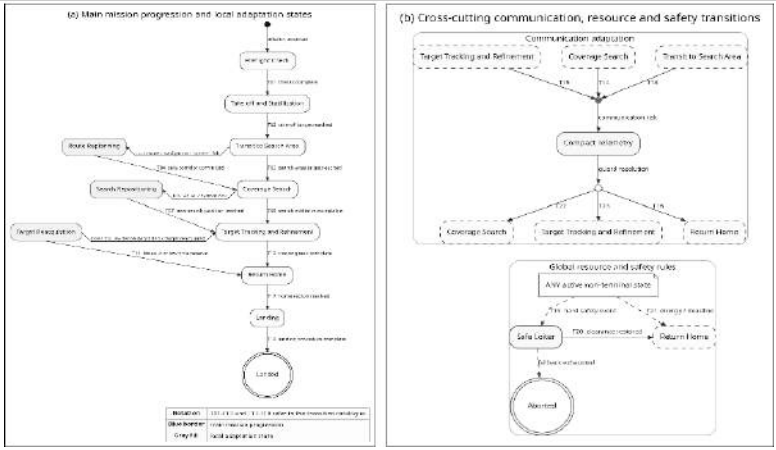


Figure 1. Declarative graph of the multistage mission: (a) main sequence and local adaptation states; (b) cross-cutting communication, resource, and safety transitions.

The primary scenario set $S_{main} = \{S0, ..., S7\}$ verifies nominal execution, isolated degradations, and a mixed-initiative conflict. A separate set $S_{safe} = \{V1, V2\}$ is used to validate safety transitions. The experimental scenarios are described in Table 1.

Table 1

Scenarios of the multi-run simulation experiment for unmanned-mission execution

ID	Scenario	Graph aspect under test
S0	Nominal mission	Reference execution of the nominal and optional branches
S1	Communication degradation	T13–T16/T22–T23 communication-adaptation branch
S2	Operator overload	Shared-routing and global return rule T21
S3	Computational overload	System-risk branch T03–T04 and processing-time suitability
S4	Visual occlusion	Search/tracking evidence and adaptive visual branches
S5	Energy constraint	Energy evidence and resource return rule T21
S6	Mixed-initiative conflict	Operator initiative within graph-constrained routing
S7	Compound degradation	Joint channel degradation and fallback competition
V1	Proximity hazard during search	Explicit safety transition T19 during the search segment
V2	Actuator fault during return	Explicit safety transition T19 during return

Ten runs with independent seeds were performed for each scenario. The base simulation step is 0.5 s; however, execution terminates earlier upon reaching LANDED or ABORTED, or upon reaching the 75-second mission limit. At every step, the active state, selected transition, its criticality, $\sum$, R_{eff} , control mode, fallback, channel estimates, events, physical progress, and safety indicators are logged.

6. Experimental evaluation and performance assessment

The results are analyzed in three interrelated dimensions: mission completion, activation of the declarative graph edges, and phase-dependent control-mode selection. The nominal scenario, visual occlusion, energy constraint, and V2 ended in landing in every run (Figure 2). The partial success of the other scenarios is explained by reaching the time limit in Landing or Return. Final progress is therefore interpreted together with terminal_phase: a value close to one is not treated as LANDED unless the landing guard has been satisfied.

Mean reactivity decreases from 0.624 in S0 to 0.512 in S7, while the fifth percentile decreases from 0.345 to 0.133. This decrease does not automatically trigger SAFE: the SAFE share is zero in S0–S7 because these scenarios contain no hard safety trigger. Communication degradation and operator overload increase the share of shared routing, whereas the nominal and system-computational scenarios are executed predominantly in AUTO (Table 2).

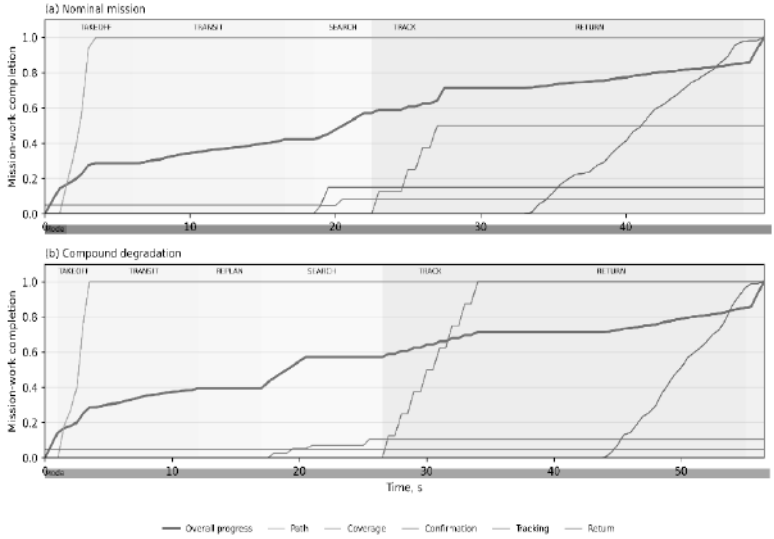


Figure 2. Mission-conditioned execution dynamics: phases, physical progress components, and control modes in the nominal (a) and compound (b) scenarios.

V1 triggered SAFE in nine of ten runs: one run did not reach the state in which the injection was scheduled before the time limit expired. Recovery through T20 (safe_loiter → return_home) was recorded in all nine episodes. V2 reached active RETURN in every run; therefore, T19 (* → safe_loiter) and T20 were activated ten times. The entry latency in both scenarios equals one

dispatcher step under the adopted discretization, and no safety-envelope violations were recorded.

Table 2

Reactivity and Mode Shares by Scenario

ID	Mean R_{eff}	P05 R_{eff}	Mean OJ	Shared	Auto	SAFE	Switches
S0	0,624	0,345	0,819	0,321	0,679	0,000	0,7
S1	0,583	0,269	0,813	0,510	0,490	0,000	0,7
S2	0,591	0,261	0,816	0,710	0,290	0,000	0,3
S3	0,536	0,155	0,798	0,320	0,680	0,000	0,7
S4	0,579	0,253	0,813	0,612	0,388	0,000	0,4
S5	0,593	0,265	0,812	0,319	0,681	0,000	0,7
S6	0,588	0,207	0,815	0,612	0,388	0,000	0,4
S7	0,512	0,133	0,797	0,514	0,486	0,000	0,5
V1	0,594	0,251	0,810	0,493	0,471	0,035	2,2
V2	0,617	0,332	0,816	0,243	0,721	0,036	2,7

Panel (a) of Figure 3 shows that channel evidence retains local interpretability for the principal isolated effects. Communication evidence decreases most strongly in S1, operator evidence in S2, system-computational evidence in S3, and visual evidence in S4. S7 simultaneously reduces the operator, communication, visual, and system components, corresponding to compound degradation. At the same time, S5 does not produce a dominant reduction in energy evidence within the 75-second horizon; the largest shift occurs in the operator channel. RQ1 is therefore only partially supported, and the energy loop requires a longer or more targeted scenario.

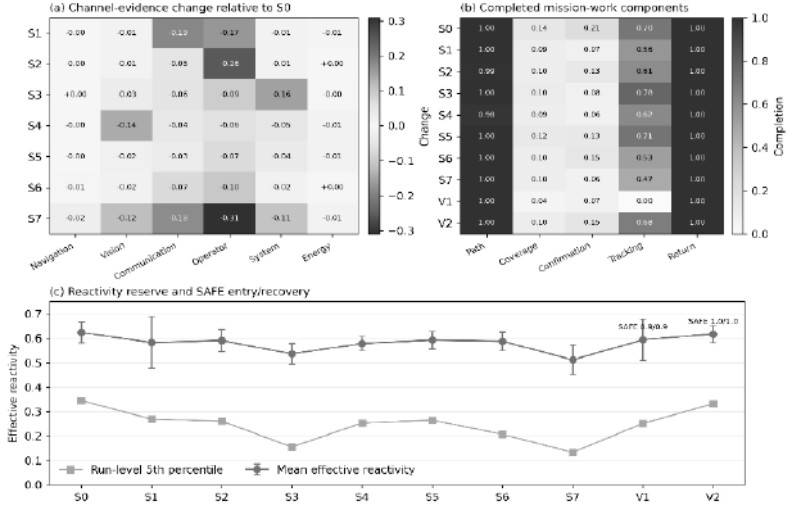


Figure 3. Cross-scenario evidence for multimodality (a), mission progress (b), and reactive suitability (c).

Panel (b) of Figure 3, together with Figure 2, shows that the current graph state determines the available outgoing transitions, while the selected transition determines the relevant channel evidence and admissible event routes. Thus, mission context

affects delegation before modes are compared. In all scenarios, the route component and return are close to full completion, whereas confirmation and tracking are substantially more sensitive to channel quality. The terminal state is considered separately from integral progress: a progress value close to one does not replace the fact that the transition to LANDED has been executed. Panel (c) of Figure 3 shows a reduction in the reactive margin without conflating degradation with an emergency mode. No hard-deadline misses, soft violations, or safety-envelope violations occur throughout the series. SAFE is activated only in V1 and V2; the number of entries equals the number of recoveries for the episodes that actually occurred. RQ3 is therefore supported within the simulation setting.

Panel (a) of Figure 4 summarizes conflicting operator requests in S6 and S7. In S6, 57 explicit decisions were recorded: 54 override and 3 defer; in S7, 13 decisions were recorded: 12 override and 1 defer. The current stochastic series does not include a separate compatible-initiative scenario; therefore, the absence of accept decisions should not be interpreted as evidence that the corresponding branch is inoperative. The experiment confirms filtering of conflicting initiative, but RQ4 is supported only partially overall. Full validation requires an additional scenario in which the operator request is structurally and statistically admissible.

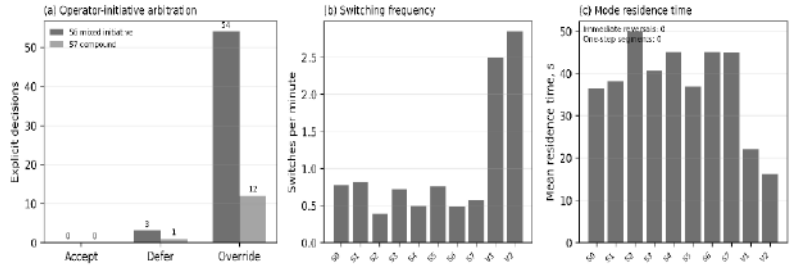


Figure 4. Operator-initiative arbitration and delegation stability: decisions, switching frequency, and residence time.

Panels (b)–(c) of Figure 4 show that, in S0–S7, the mean number of switches is 0.3–0.7 per run and the mean dwell time is approximately 36–50 s. The number of switches is naturally higher in V1 and V2 because each safety episode adds an entry into SAFE and a recovery. Across all ten scenarios, the number of immediate reverse switches and one-step mode segments is zero. Thus, statistical mode comparison and residence time suppress oscillations without blocking meaningful safety transitions. RQ5 is therefore experimentally supported.

7. Conclusions and Prospects

This article presents an integrated mission-oriented model of hybrid control for a robotic system in which event-driven reactivity, multimodal channel evidence, semantic state, the mission graph, operator initiative, safety constraints, and the delegation policy are combined into a single sequence of formal policies. The proposed model defines shared control through event routing among the signal, feature, mission, operator, autonomous, and safety processing levels. Consequently, the control mode is determined by the event class, active mission transition, time budget, channel state, operator availability, reactive suitability, and mission-

execution safety conditions. An additional element of novelty is the decomposition of the robotic system's multimodal state into channel evidence containing a channel-state estimate, data freshness, and evidence uncertainty. This representation preserves the physical meaning of the navigation, visual, communication, operator, system-computational, and energy channels and enables their subsequent semantic interpretation in the context of the active mission phase. On this basis, the concept of mode-dependent effective reactivity $R_{eff}(j,q,k)$ is introduced; it determines the admissibility of a specific control mode for the active mission transition with consideration of event deadlines, routing, operator or autonomous participation, and safety/fallback logic. The proposed model provides a consistent basis for analyzing mission progress, reactive admissibility, operator intervention, channel conflict, and delegation stability under degradation of individual modalities.

Phase-level analysis confirms the central proposition: the significance of a channel is determined by the transition context. Communication and operator evidence are most critical for CONFIRM; visual evidence is most critical for SEARCH and TRACK; system-computational availability contributes to all reactive transitions; and energy evidence determines whether the plan continues or an energy return is initiated. Consequently, the mode changes with mission semantics even under a similar overall channel state.

Further work should include targeted scenarios, platform-in-the-loop and hardware-in-the-loop re-identification, and automatic generation of SCXML/UPPAAL representations from the same mission description file.

References

[1] Dellermann, D., Ebel, P., Söllner, M., & Leimeister, J. M. (2019). Hybrid intelligence. *Business & Information Systems Engineering*, *61*(5), 637-643. DOI: 10.1007/s12599-019-00595-2.

[2] Yarmilko, A., & Marchenko, S. (2026). Conceptual model of hybrid control of robotic systems with delegation of authority. In *Conference Proceedings of the VIII International Scientific-Practical Conference "Information Technology for Education, Science and Technics" (ITEST-2026)* (pp. 420-422). Cherkasy, Ukraine: ChSTU. DOI: 10.5281/zenodo.21843513.

[3] Campbell, J. M. (2021). *Psychological effects on UAV operators and proposed mitigation strategies to combat PTSD*. (Master's thesis). Naval Postgraduate School, Monterey, CA. URL: https://apps.dtic.mil/sti/trecms/pdf/AD1150884.pdf.

[4] Kieffer, J. W., & Stahlman, S. (2021). Mental health disorders, behavioral health problems, fatigue and sleep outcomes in remotely piloted aircraft/manned aircraft pilots, and remotely piloted aircraft crew, U.S. Air Force, 1 October 2003-30 June 2019. *Medical Surveillance Monthly Report*, *28*(8), 14-21. PMID: 34622757.

[5] Goodrich, M. A., & Schultz, A. C. (2007). Human-robot interaction: a survey. *Foundations and Trends in Human-Computer Interaction*, *1*(3), 203-275. DOI: 10.1561/1100000005.

[6] Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man, and Cybernetics* – Part A: *Systems and Humans*, *30*(3), 286-297. DOI: 10.1109/3468.844354.

[7] Singh, S., Rantanen, E., & Heard, J. (2026). Human-robot teaming: A comprehensive survey on collaboration, communication and cognition. *ACM Transactions on Human-Robot Interaction*, *15*(2), 43. DOI: 10.1145/3776548.

[8] Dragan, A. D., & Srinivasa, S. S. (2013). A policy-blending formalism for shared control. *The International Journal of Robotics Research*, *32*(7), 790-805. DOI: 10.1177/0278364913490324.
[9] Javdani, S., Admoni, H., Pellegrinelli, S., Srinivasa, S. S., & Bagnell, J. A. (2018). Shared autonomy via hindsight optimization for teleoperation and teaming. *The International Journal of Robotics Research*, *37*(7), 717-742. DOI: 10.1177/0278364918776060.
[10] Reddy, S., Dragan, A. D., & Levine, S. (2018). Shared autonomy via deep reinforcement learning. *Robotics: Science and Systems, XIV*. DOI: 10.15607/RSS.2018.XIV.005.
[11] Lee, J., Balachandran, R., Singh, H., Feng, J., Mishra, H., De Stefano, M. … Kondak, K. (2026). SPIRIT: Perceptive shared autonomy for robust robotic manipulation under deep learning uncertainty. *arXiv:2603.05111*. DOI: 10.48550/arXiv.2603.05111.
[12] Luckcuck, M., Farrell, M., Dennis, L. A., Dixon, C., & Fisher, M. (2019). Formal specification and verification of autonomous robotic systems: A survey. *ACM Computing Surveys*, *52*(5), 100. DOI: 10.1145/3342355.
[13] Menghi, C., Tsigkanos, C., Pelliccione, P., Ghezzi, C., & Berger, T. (2024). Mission specification patterns for mobile robots. *IEEE Transactions on Software Engineering*, *50*(11), 2992-3022. DOI: 10.1109/TSE.2024.3453601.
[14] Qian, H., Wang, M., Zhu, M., & Wang, H. (2025). A review of multi-sensor fusion in autonomous driving. *Sensors*, *25*(19), 6033. DOI: 10.3390/s25196033.
[15] Han, X., Chen, S., Fu, Z., Feng, Z., Fan, L., An, D. … Xu, S. (2025). Multimodal fusion and vision-language models: A survey for robot vision. *Information Fusion*, *126*(PB), 103327. DOI: 10.1016/j.inffus.2025.103327.
[16] Julier, S. J., & Uhlmann, J. K. (2004). Unscented filtering and nonlinear estimation. *Proceedings of the IEEE*, *92*(3), 401-422. DOI: 10.1109/JPROC.2003.823141.
[17] Doucet, A., de Freitas, N., & Gordon, N. (2001). An introduction to sequential Monte Carlo methods. In *Sequential Monte Carlo methods in practice* (pp. 3-14). New York: Springer. DOI: 10.1007/978-1-4757-3437-9_1.
[18] Yin, Z., & Zhang, J. (2014). Recognition of mental workload levels under complex human-machine collaboration by using physiological features and adaptive support vector machines. *IEEE Transactions on Human-Machine Systems*, *44*(2), 200-214. DOI: 10.1109/THMS.2013.2295853.
[19] Charles, R. L., & Nixon, J. (2019). Measuring mental workload using physiological measures: A systematic review. *Applied Ergonomics*, *74*, 221-232. DOI: 10.1016/j.apergo.2018.08.028.
[20] Liu, C. L., & Layland, J. W. (1973). Scheduling algorithms for multiprogramming in a hard-real-time environment. *Journal of the ACM*, *20*(1), 46-61. DOI: 10.1145/321738.321743.
[21] Lehoczky, J. P., Sha, L., & Ding, Y. (1989). The rate monotonic scheduling algorithm: Exact characterization and average case behavior. In *Proceedings of the IEEE Real-Time Systems Symposium* (pp. 166-171). DOI: 10.1109/REAL.1989.63567.
[22] Bernat, G., Burns, A., & Liamosi, A. (2001). Weakly hard real-time systems. *IEEE Transactions on Computers*, *50*(4), 308-321. DOI: 10.1109/12.919277.
[23] Salamun, K., Pavić, I., Džapo, H., & Čuljak, I. (2023). Weakly hard real-time model for control systems: A survey. *Sensors*, *23*(10), 4652. DOI: 10.3390/s23104652.
[24] Liubimov, O., Turkin, I., Cheranovskiy, V., & Volobuieva, L. (2024). UAV mission computer operation mode optimization focusing on computational energy efficiency and system responsiveness. *Computation*, *12*(12), 235. DOI: 10.3390/computation12120235.
[25] Hsu, K.-C., Hu, H., & Fisac, J. F. (2024). The safety filter: A unified view of safety-critical control in autonomous systems. *Annual Review of Control, Robotics, and Autonomous Systems*, *7*, 47-72. DOI: 10.1146/annurev-control-071723-102940.
[26] Garg, K., Usevitch, J., Breeden, J., Black, M., Agrawal, D., Parwana, & H. Panagou, D. (2024). Advances in the theory of control barrier functions: Addressing practical challenges

in safe control synthesis for autonomous and robotic systems. *Annual Reviews in Control*, *57*, 100945. DOI: 10.1016/j.arcontrol.2024.100945.

[27] Schierman, J. D., DeVore, M. D., Richards, N. D., & Clark, M. A. (2020). Runtime assurance for autonomous aerospace systems. *Journal of Guidance, Control, and Dynamics*, *43*(12), 2205-2218. DOI: 10.2514/1.G004862.

МОДЕЛІ ГІБРИДИЗАЦІЇ ЛЮДИНО-МАШИННОГО УПРАВЛІННЯ РОБОТИЗОВАНИМИ СИСТЕМАМИ

Ph.D., Ярмілко А., Марченко С.

Черкаський національний університет імені Богдана Хмельницького, Україна

Анотація. *У статті представлено структуровану мультимодальну орієнтовану на виконання місії модель гібридного керування роботизованими системами, що функціонують в умовах неповної інформації, змінної якості каналів зв'язку, обмежень реального часу та участі оператора. На відміну від традиційних методів поєднання команд або стратегій, спільне керування організовано шляхом маршрутизації допустимих подій між модулями обробки, що відповідають за дії оператора, автономну роботу, виконання місії та безпеку. Мультимодальний стан системи охоплює навігаційний, візуальний, комунікаційний, операторський, системно-обчислювальний та енергетичний канали. Модель було перевірено з використанням синтетичних даних у середовищі імітаційного моделювання з дискретним часом для декларативно визначеної багатоетапної місії. Результати продемонстрували залежність значущості каналів від контексту, коректні переходи між етапами місії та резервними режимами, відхилення суперечливих ініціатив оператора, а також стабільне делегування функцій між ручним, спільним, автономним та орієнтованим на безпеку режимами.*

Ключові слова. *Гібридне керування; роботизовані системи; граф місії; спільна автономність; маршрутизація подій; мультимодальне злиття даних; ефективна реактивність; ініціатива оператора; резервний режим безпеки*

Section 3 Digital platforms, security, and ICT infrastructure

УДК004.932:004.896
DOI

СИСТЕМА 3D-КОМП'ЮТЕРНОГО ЗОРУ ДЛЯ АВТОМАТИЗОВАНОГО ЗАХОПЛЕННЯ ТА СОРТУВАННЯ ВІДХОДІВ МОБІЛЬНИМИ РОБОТАМИ

Ph.D., Бойко Н. [0000-0002-6962-9363]

Національний університет «Львівська політехніка», Україна,
Львівський національний університет ветеринарної медицини та біотехнологій імені С. З. Ґжицького, Україна
EMAIL: Nataliya.i.boyko@gmail.com

Анотація. *У статті розроблено та досліджено систему 3D-комп'ютерного зору для підвищення операційної ефективності та точності маніпуляцій автономних прибиральних робототехнічних комплексів під час збору неструктурованого сміття довільної форми. Запропоновано синергетичний підхід, який усуває потребу в ресурсоємних тривимірних нейромережах за рахунок поєднання швидкодійного одноетапного детектора YOLOv5 із методами обчислювальної геометрії. Нейромережеву модель донавчено на спеціалізованому наборі даних TACO для локалізації та класифікації відходів у режимі реального часу на колірному растрі. На основі даних RGB-D-сенсора Intel Real Sense D435, відфільтрованих методом медіанного абсолютного відхилення, реалізовано алгоритм сканування Грехема для побудови опуклої оболонки та метод обертових каліперів для формування мінімального орієнтованого прямокутника. Це дозволяє детерміновано обчислювати 3D-центроїд, геометричні габарити та орієнтацію головної осі об'єкта. Сформовано математичну модель розрахунку 6-DoF пози захоплення* $T_{grasp} \in SE(3)$ *з урахуванням кінематичних і фізичних обмежень захоплення маніпулятора та розроблено індекс пріоритетності прибирання. Програмну інтеграцію перцептивного конвеєра здійснено у середовищі ROS 2. Експериментальні дослідження підтвердили високу ефективність розробленого рішення: підсумкова обчислювальна затримка становить близько* $\approx 50мс(\approx 20Гц)$*, а точність маніпуляцій досягає 89,1% успішних захоплень. Запропонований комплекс мінімізує кількість «промахів» і готовий до впровадження в автономні мобільні роботи-прибиральники.*

Ключові слова: *3D-комп'ютерний зір, маніпуляційне захоплення, YOLOv5, метод обертових каліперів, сканування Грехема, 6-DoF поза, ROS 2.*

1 Вступ

В умовах сучасного розвитку суспільства, стрімкої урбанізації та зростання чисельності населення проблеми накопичення та ефективного управління відходами набувають критичного значення. Традиційні підходи до збору та сортування сміття, що базуються на ручній праці, є не лише неефективними та повільними, але й становлять суттєві ризики для здоров'я робітників через контакт із токсичними або небезпечними речовинами [4, 10].

Впровадження автономних робототехнічних комплексів у сферу обслуговування та прибирання є перспективним шляхом вирішення цієї проблеми [3]. Проте одна з основних технологічних перешкод на цьому шляху

– відсутність у роботів здатності ефективно взаємодіяти з неструктурованими та довільними за формою об'єктами. Більшість сучасних систем комп'ютерного зору здатні успішно виявляти об'єкти на плоских 2D-зображеннях за допомогою обмежувальних рамок – bounding boxes, але цього недостатньо для фізичного маніпулювання: робот повинен знати точні 3D-координати, просторову орієнтацію та фізичні межі об'єкта для надійного захоплення.

Саме тому розробка інтегрованих алгоритмів, які поєднують глибоке навчання для детекції сміття із просторовим 3D-моделюванням та обчислювальною геометрією для вибору точної точки підйому, є надзвичайно актуальним завданням на стику робототехніки, комп'ютерного зору та штучного інтелекту.

Наукова новизна одержаних результатів полягає у створенні концептуально нового інтегрованого підходу до автоматизованого визначення просторового положення та точок захоплення неструктурованих об'єктів довільної форми. У роботі вперше запропоновано синергетичну модель, яка поєднує можливості глибокого навчання нейромережі YOLOv5 для швидкої детекції й класифікації сміття з алгоритмами обчислювальної геометрії, зокрема алгоритмом обертових каліперів та скануванням Грехема для формування мінімального охоплюючого прямокутника.

Практична цінність дослідження полягає у створенні готового програмно-алгоритмічного комплексу, орієнтованого на безпосереднє впровадження у робототехнічні системи автономного прибирання для роботи в закритих приміщеннях і на відкритих територіях.

Запропоноване рішення розв'язує критичну проблему неефективних спроб захоплення та «промахів» маніпулятора під час збору сміття за рахунок точного розрахунку координатного центру підйому, адаптованого під фізичні можливості робочого органу.

Враховуючи актуальність проблеми, її практичну спрямованість та необхідність реалізації окресленої наукової новизни, метою дослідження є підвищення операційної ефективності та точності маніпуляцій автономних прибиральних робототехнічних комплексів шляхом розробки та впровадження інтегрованого алгоритмічного підходу, який поєднує можливості YOLOv5 та методів обчислювальної геометрії для точного визначення 3D-координат, просторової орієнтації та оптимальної точки підйому неструктурованого сміття довільної форми. Для досягнення поставленої мети передбачено послідовне вирішення низки взаємопов'язаних науково-прикладних завдань.

Насамперед здійснюється поглиблений аналіз існуючих підходів у галузі комп'ютерного зору, 3D-моделювання та обчислювальної геометрії для виявлення найбільш ефективних методів розпізнавання й захоплення об'єктів довільної форми.

На наступному етапі формується та готується спеціалізований набір даних побутового й промислового сміття, необхідний для подальшого навчання та оптимізації нейромережевої моделі YOLOv5, що має забезпечити високу точність детектування й класифікації відходів у режимі реального часу.

У свою чергу, ключовим теоретико-алгоритмічним завданням виступає розробка синергетичного методу обчислювальної геометрії, який на основі

даних RGB-D сенсора, алгоритму сканування Грехема та методу обертових каліперів здійснює побудову мінімального захоплюючого прямокутника для обчислення геометричного центру й просторової орієнтації об'єкта. Паралельно формується методика визначення точних 3D-координат точки підйому, адаптована до кінематичних і фізичних обмежень маніпулятора робота. Завершальний блок завдань передбачає програмну інтеграцію розробленого комплексу в систему керування робототехнічною платформою та проведення серії експериментальних досліджень для оцінки точності розрахунку точок підйому, мінімізації кількості «промахів» і підтвердження практичної ефективності запропонованого рішення.

2 Огляд наявних аналогів та аналіз сучасного стану досліджень

Автоматизація процесів моніторингу, детекції та збору твердих побутових і виробничих відходів за допомогою автономних робототехнічних комплексів є критично важливим завданням сучасного міського господарства та промисловості [1, 2]. Впровадження інтелектуальних мобільних систем дозволяє не лише знизити частку небезпечної ручної праці та мінімізувати біологічні ризики для персоналу, а й суттєво підвищити оперативність прибирання неструктурованих приміщень і відкритих територій [3, 4, 5].

Ефективність функціонування автономного робота-збирача визначається якістю роботи його перцептивної підсистеми (комбінації сенсорів та алгоритмів комп'ютерного зору), а також точності орієнтування захоплення маніпулятора відносно знайдених об'єктів.

Проведений систематичний огляд науково-технічної літератури дозволив розділити наявні рішення за технічним інструментарієм та функціональним призначенням на три ключові категорії:

1. Мобільні робототехнічні системи прибирання та навігації: автори [2, 3, 4, 6, 7] висвітлюють створення автономних платформ (зокрема на базі фреймворку ROS та рішень AIoT) для локалізації сміття у закритих приміщеннях, на газонах чи біля контейнерних майданчиків. Застосування реконфігурованих роботів, наприклад, hTetro [6] забезпечує високу захоплення території, проте питання точного розрахунку просторової пози захоплення (6-DoF) в більшості цих робіт залишається поза увагою.

2. Нейромережеві методи 2D-детекції та класифікації відходів: в роботах [4, 8, 11, 12] розглянуто застосування згорткових нейронних мереж (Faster R-CNN, VGG-16, SSD, YOLOv4/YOLOv4-Tiny) для ідентифікації типів сміття. Більшість із них обмежується побудовою двовимірних обмежувальних рамок (2D Bounding Boxes), що дає можливість виявити наявність об'єкта в кадрі, але не забезпечує достатньої інформації для орієнтації механічного захоплення в 3D-просторі.

3. Алгоритми обробки сенсорних даних та перцепції середовища: дослідження [13, 14] присвячені обробці даних часових рядів на крайніх пристроях (Edge Computing) та класичним геометричним алгоритмам виявлення перешкод на основі 2D LiDAR (DBSCAN, DFS). Вони забезпечують безпеку переміщення робота, проте не вирішують завдання 3D-профілювання об'єктів довільної форми. Систематизовані результати порівняльного аналізу наявних аналогів наведено в Табл. 1.

Таблиця 1.

Огляд та порівняльний аналіз існуючих аналогів

№	Назва дослідження	Технічний інструментарій (сенсори)	Цільове завдання
1	A vision-based robotic grasping system using deep learning for garbage sorting [4]	RPN, VGG-16	Детекція та сортування сміття для робототехнічного захоплення
2	A Review of Trash Collecting and Cleaning Robots [5]	Scopus, GoogleScholar	Систематичний огляд автономних роботів для збору та прибирання сміття
3	Optimal selective floor cleaning using deep learning algorithms and reconfigurable robot hTetro [6]	CCTV, SORT, SSD	Визначення оптимальних зон прибирання та детекція відходів роботом hTetro
4	Design and Implementation of an Artificial Intelligence of Things-Based Autonomous Mobile Robot System for Cleaning Garbage [7]	ROS, AIoT	Автоматизація збору сміття з контейнерів мобільним роботом
5	OATCR: Outdoor Autonomous Trash-Collecting Robot Design Using YOLOv4-Tiny [8]	YOLOv4-Tiny, Mask R-CNN	Розробка автономного робота для збору сміття у відкритому середовищі
6	Autonomous Trash Collector Based on Object Detection Using Deep Neural Network [9]	ROS, RNN, YOLOv4	Створення малогабаритного автономного робота-збирача сміття
7	Deep Learning Based Robot for Automatically Picking Up Garbage on the Grass [10]	ROS, DeepLearning	Детекція сміття та навігація робота на трав'янистому покритті
8	Cascaded Machine-Learning Technique for Debris Classification in Floor-Cleaning Robot Application [11]	CNN, SVM, SSD	Каскадна класифікація відходів підлоги та оцінка можливості підйому
9	Deep Learning Based Pavement Inspection Using Self-Reconfigurable Robot [12]	DCNN, MMS	Детекція дефектів дорожнього покриття та відходів
10	A cascade ensemble-learning model for the deployment at the edge: case on missing IoT data recovery in environmental monitoring systems [13]	Edgecomputing, SVR	Відновлення втрачених IoT-даних, детекція аномалій та зменшення розмірності
11	An Obstacle-Finding Approach for Autonomous Mobile Robots Using 2D LiDAR Data [14]	2D LiDAR, DFS, DBSCAN	Детекція перешкод на основі лидарних даних для мобільних роботів

Аналіз наведених джерел [6-16] дозволяє виділити такі критичні недоліки та обмеження існуючих рішень:

– Обчислювальний дисбаланс та затримка інференсу: Застосування важких двоетапних моделей (VGG-16 [4], Mask R-CNN [8]) або обчислювально містких 3D-згорткових мереж вимагає значних обчислювальних ресурсів, що є проблематичним для бортових контролерів роботів і призводить до високих затримок $(>100мс)$.

– Відсутність точного розрахунку пози захоплення (6-DoF): Більшість аналогів [6, 9, 11] обмежуються 2D-локалізацією. При роботі з об'єктами

довільної та неструктурованої форми це спричиняє значну кількість «промахів» маніпулятора через відсутність даних про орієнтацію головних осей симетрії об'єкта.

– Недостатня стійкість до зашумлених даних карт глибини: Пряма обробка 3D-хмар точок без попередньої високошвидкісної 2D-фільтрації є вразливою до артефактів зчитування RGB-D сенсорів.

Отже, існує чітка потреба в розробці гібридного методу, який би поєднував швидкодію сучасних 2D-детекторів таких як YOLOv5 із математично ефективними підходами обчислювальної геометрії. Це дозволить здійснювати детермінований розрахунок 3D-центроїда та векторів орієнтації захоплення $T_{grasp} \in SE(3)$ без використання важких 3D-нейромереж, забезпечуючи високу точність та роботу перцептивного конвеєра в режимі реального часу.

3 Огляд методів комп'ютерного зору для виявлення та класифікації сміття

3.1 Методи 2D-детекції та класифікації відходів (Класичні CV-методи vs CNN: Faster R-CNN, YOLOv5)

Для розв'язання задачі локалізації та класифікації відходів у цифровому відеопотоці в сучасній теорії комп'ютерного зору застосовують дві основні парадигми: класичні аналітичні методи обробки зображень та згорткові нейронні мережі (CNN) [10, 13]. Традиційні підходи комп'ютерного зору базуються на ручному конструюванні ознак (feature engineering). Сегментація за кольором реалізується шляхом переведення вхідного RGB-зображення в колірну модель HSV (Hue, Saturation, Value) та порогової фільтрації у визначеному діапазоні (1) [2, 5]:

$$I_{bin}(x,y) = \begin{cases} 1 & якщо\ H(x,y) \in [H_{\min}, H_{\max}] \wedge S(x,y) \in [S_{\min}, S_{\max}] \wedge V(x,y) \in [V_{\min}, V_{\max}], \\ & 0 \end{cases} \quad (1)$$

Для виділення контурів об'єктів використовується градієнтний оператор Кенні (Canny edge detector). Величина $|\nabla I(x,y)|$ та орієнтація $\alpha(x,y)$ градієнта інтенсивності обчислюються через часткові похідні по осях [2, 3, 9]:

$$|\nabla I(x,y)| = \sqrt{G_x^2 + G_y^2}, \alpha(x,y) = \arctan\left(\frac{G_y}{G_x}\right), \quad (2)$$

де $G_x = K_x * I$, $G_y = K_y * I$ – згортка зображення I з ядрами Собеля K_x, K_y.

Виділення ключових точок та опис текстур реалізується через розрахунок дескрипторів SIFT, SURF або ORB. Для дескриптора SIFT обчислюється гістограма орієнтацій градієнтів у околі локального екстремуму функції різниці гаусіанів $DoG(x,y,\sigma) = L(x,y,k\sigma) - L(x,y,\sigma)$, створюючи 128-вимірний вектор дескриптора $d \in R^{128}$. Порівняння об'єктів здійснюється через обчислення евклідової відстані $\|d_1 - d_2\|_2$. Головними недоліками традиційних методів є висока чутливість до змін освітлення, текстури підстильної поверхні, оклюзій (occlusions) та нелінійних деформацій об'єктів (зім'ята банка, рваний папір), що робить їх непридатними для обробки неструктурованого сміття. Альтернативою є методи глибокого навчання (Deep Learning), де детекція

розглядається як задача математичного відображення $f_\Theta : R^{H\times W\times 3} \to O$, де $O = \{(B_k, c_k, p_k)\}_{k=1}^{K}$ – множина знайдених об'єктів, а Θ – вектор параметрів згорткової нейронної мережі [8]. Двоетапні детектори (Two-stage detectors, наприклад Faster R-CNN) розділяють задачу на генерацію регіонів інтересу (Region Proposal Network, RPN) та їх подальшу класифікацію з регресією координат. RPN мінімізує функцію втрат (3) [3, 10]:

$$L_{RPN}(\{p_i\},\{t_i\}) = \frac{1}{N_{cls}}\sum L_{cls}(p_i, p_i^*) + \lambda\frac{1}{N_{reg}}\sum p_i^* L_{reg}(t_i, t_i^*), \quad (3)$$

де p_i – ймовірність наявності об'єкта в i-му анкорі, p_i^* - істинна мітка, t_i та t_i^* - вектори параметризованих координат обмежувальної рамки, L_{cls} – логарифмічні втрати класифікації, а L_{reg} – згладжена L_1-втрата (Smooth L_1). Попри високу точність, висока обчислювальна складність двоетапних систем обмежує частоту обробки кадрів (< 10 FPS), що є неприйнятним для бортових систем робота в режимі реального часу.

Одноетапні детектори (Retina Net, серія YOLO) виконують детекцію за один прохід мережі, розбиваючи вхідний кадр на сітку $S\times S$. Архітектура YOLOv5 є найбільш ефективною для мобільних робототехнічних платформ завдяки оптимальному співвідношенню точності та обчислювальних витрат.

В основі YOLOv5 лежить регресія параметрів обмежувальної рамки відносно зумовлених анкорів (anchor boxes). Передбачені центр (b_x, b_y), ширина b_w та висота b_h Bounding Box обчислюються за формулами (4) [5]:

$$b_x = 2\sigma(t_x) - 0.5 + c_x;\ b_y = 2\sigma(t_y) - 0.5 + c_y;\ b_w = p_w(2\sigma(t_w))^2;\ b_h = p_h(2\sigma(t_h))^2, \quad (4)$$

де $\sigma(x) = \frac{1}{1+e^{-x}}$ – сигмоїдна функція, (c_x, c_y) – координати верхнього лівого кута комірки сітки, p_w, p_h - початкові розміри анкора, а t_x, t_y, t_w, t_h - вихідні значення відповідного шарнірного шару нейромережі.

Навчання YOLOv5 здійснюється шляхом мінімізації комбінованої функції втрат L_{YOLO}, що складається з трьох компонентів (5) [4]:

$$L_{YOLO} = \lambda_{box}L_{CIoU} + \lambda_{obj}L_{obj} + \lambda_{cls}L_{cls}. \quad (5)$$

Компонента регресії рамок L_{CIoU} базується на метриці Complete Intersection over Union (CIoU), яка враховує площу перекриття, відстань між центрами та співвідношення сторін (6) [7]:

$$L_{CIoU} = 1 - IoU + \frac{\rho^2(b, b^{gt})}{c^2} + \alpha v, \quad (6)$$

де $IoU = \frac{|B\cap B^{gt}|}{|B\cup B^{gt}|}$, $\rho(\cdot)$- евклідова відстань між центрами передбаченої b а еталонної b^{gt} рамок, c – діагональ найменшого прямокутника, що охоплює обидві рамки. Ваговий коефіцієнт α та параметр узгодженості пропорцій v визначаються як (7) [5]:

$$\alpha = \frac{v}{(1-IoU)+v}, \quad v = \frac{4}{\pi^2}\left(\arctan\frac{w^{gt}}{h^{gt}} - \arctan\frac{w}{h}\right)^2. \tag{7}$$

Втрати об'єктивності L_{obj} та класифікації L_{cls} розраховуються за допомогою бінарної крос-ентропії (*BCE Loss*) (8) [6]:

$$L_{BCE}(y,\hat{y}) = -\left[y\log\sigma(\hat{y}) + (1-y)\log(1-\sigma(\hat{y}))\right]. \tag{8}$$

Висока швидкість інференсу YOLOv5 (> 30 FPS на бортових GPU) та підтримка оптимізацій через формати TensorRT, ONNX, Open VINO дозволяють виконувати нейромережевий аналіз у режимі реального часу. Проте ключовою проблемою залишається статистичний зсув даних (domain shift): стандартні набори даних характеризуються розподілом правильних, неідеалізованих об'єктів $P_{COCO}(X)$, який суттєво відрізняється від розподілу реально деформованих та забруднених відходів $P_{waste}(X)$. Це робить критично необхідним збір, розмітку та адаптацію спеціалізованого набору даних побутового й промислового сміття.

3.2 Методи 3D-визначення позицій для захоплення

Після успішного виконання 2D-локалізації та класифікації об'єкта за допомогою нейромережі виникає задача визначення його просторових 3D-координат та оптимальної пози захоплення (Grasp Pose) для робочого органу маніпулятора. Наявні у науково-технічній літературі підходи до розв'язання цієї задачі поділяються на end-to-end нейромережеві системи та комбіновані геометрично-евристичні алгоритми. Підходи першої категорії, зокрема Grasp Net та Dex-Net, оперують безпосередньо тривимірною хмарою точок $P \in R^{N\times 3}$ що генерується RGB-D сенсором. Задача зводиться до максимізації функції оцінки якості захоплення $Q(P,g)$ (9) [2]:

$$g^* = \arg\max_g Q(P,g), \tag{9}$$

де параметр захоплення $g = (R,t,w)$ містить матрицю повороту $R \in SO(3)$, вектор трансляції $t \in R^3$ та величину розкриття губок захвату w.

Процес оцінки передбачає застосування тривимірних згорткових мереж (PointNet++, EdgeConv) для розрахунку характеристик кожної точки (10) [6]:

$$h_i^{l+1} = \max_{j\in N(i)} h_\Theta\left(h_i^{(l)}, h_j^{(l)} - h_i^{(l)}\right), \tag{10}$$

де $N(i)$ - k -найближчих сусідів точки p_i, а h_Θ – нелінійна апроксимаційна функція нейромережі.

Основними недоліками End-to-End нейромережевих підходів є:

1. Висока обчислювальна складність алгоритмів вибірки k -найближчих сусідів $(O(N\log N))$ або $O(N^2)$, що зумовлює тривалий час інференсу $t_{\text{inf}} > 100мс$.
2. Потреба у мільйонних наборах даних із розміченими 3D-граспами.
3. Низька стійкість до артефактів карти глибини (відсутність даних на прозорих пластикових пляшках чи дзеркальних поверхнях спричиняє розрив хмари точок та хибну генерацію поз захоплення).

Альтернативним та обчислювально ефективним підходом є поєднання 2D-локалізації нейромережею YOLOv5 із геометричним аналізом відповідного регіону карти глибини. Для кожного виявленого 2D-граничного прямокутника B_k множина внутрішніх пікселів $(u,v)\in B_k$ проектується у простір камери $(X_c,Y_c,Z_c)^T$ з використанням матриці внутрішніх параметрів камери K (11) [7, 9]:

$$\begin{bmatrix} X_c \\ Y_c \\ Z_c \end{bmatrix} = Z \cdot K^{-1} \begin{bmatrix} u \\ v \\ 1 \end{bmatrix} = \begin{bmatrix} Z\dfrac{(u-c_x)}{f_x} \\ Z\dfrac{(u-c_y)}{f_y} \\ Z \end{bmatrix}, \tag{11}$$

де f_x, f_y - фокусні відстані, (c_x, c_y) – координати головної точки оптичної осі, а $Z = D(u,v)$ – значення глибини у відповідному пікселі.

Для усунення викидів (шумів сенсора, вимірів підлоги та оклюзій) застосовується робастний метод фільтрації на основі медіанного абсолютного відхилення (*MAD*). З первинного масиву глибин $D_{raw} = \{Z_i\}_{i=1}^{M}$ формується відфільтрована множина D_{filt} (12) [3]:

$$D_{filt} = \left\{ Z_i \in D_{raw} \middle| \frac{|Z_i - med(D_{raw})|}{MAD} \le k_{mad} \right\}, \tag{12}$$

де $MAD = med\left(|Z_i - med(D_{raw})|\right)$, а $k_{mad} = 2.5$ – параметричний коефіцієнт фільтрації. Підсумкова оцінка відстані до центроїда об'єкта розраховується як робастна медіана: $Z_c = med(D_{filt})$. Для визначення фізичних меж об'єкта на 2D-растрі береться множина точок контуру $C = \{(u_m, v_m)\}_{m=1}^{M}$. Точка p_0 з найменшою координатою v обирається як початкова. Усі інші точки сортуються за полярним кутом відносно p_0. Побудова опуклої оболонки H здійснюється шляхом послідовного аналізу предикату повороту (векторного добутку) для трьох послідовних точок p_1, p_2, p_3 (13) [3, 6]:

$$D(p_1, p_2, p_3) = (u_2 - u_1)(v_3 - v_1) - (v_2 - v_1)(u_3 - u_1) \le 0 \cdot \tag{13}$$

Якщо $D(p_1, p_2, p_3) \le 0$ (поворот праворуч або колінеарність), точка $D(p_1, p_2, p_3)$ вилучається зі стеку вершин опуклої оболонки як неутворююча. На основі вершин опуклої оболонки H шукається мінімальний орієнтований охоплюючий прямокутник (*OBB*). Для кожного ребра опуклого багатокутника з кутом нахилу θ_i виконується поворот системи координат (14) [6, 9]:

$$\begin{bmatrix} u_m' \\ v_m' \end{bmatrix} = \begin{bmatrix} \cos\theta_i & \sin\theta_i \\ -\sin\theta_i & \cos\theta_i \end{bmatrix} \begin{bmatrix} u_m \\ v_m \end{bmatrix}. \tag{14}$$

Площа прямокутника як функція кута повороту θ обчислюється як (15):

$$A(\theta_i) = \left(\max_m(u_m') - \min_m(u_m')\right) \cdot \left(\max_m(v_m') - \min_m(v_m')\right) \cdot \tag{15}$$

Оптимальний кут орієнтації головної осі об'єкта θ^* та його 2D-центроїд (u_c, v_c) визначаються з умови мінімізації площі (16) [3, 6]:

$$\theta^* = \arg\min_{\theta_i} A(\theta_i), \quad (u_c, v_c) = R_{-\theta^*} \begin{bmatrix} \frac{\min(u') + \max(u')}{2} \\ \frac{\min(v') + \max(v')}{2} \end{bmatrix}. \tag{16}$$

Отримані двовимірні параметри (u_c, v_c) та відфільтрована глибина Z_c проектуються у тривимірний простір базової системи координат робота P_{base} через однорідну матрицю трансформації камери $T_{base}^{cam} \in SE(3)$ (17) [3, 9]:

$$P_{base} = T_{base}^{cam} \begin{bmatrix} Z_c \frac{u_c - c_x}{f_x} \\ Z_c \frac{v_c - c_y}{f_y} \\ Z_c \\ 1 \end{bmatrix}. \tag{17}$$

Орієнтація кута ψ_{grasp} для губок маніпулятора обчислюється як сума кута орієнтації головної осі об'єкта θ^* та просторового кута нахилу камери Φ_{cam}:

$$\psi_{grasp} = \theta^* + \Phi_{cam}. \tag{18}$$

Таким чином, геометрично-евристичний підхід зменшує обчислювальну складність від $O(N^2)$ (у випадках 3D-нейромереж) до $O(M \log M)$, де M – кількість точок 2D-контуру, що забезпечує виконання розрахунків менш ніж за $5мс$. Поєднання швидкодіючого 2D-детектора YOLOv5 з математичним апаратом сканування Грехема та обертових каліперів забезпечує детермінованість, високу точність локалізації $(Accuracy > 92\%)$ та стійкість до зашумлення карти глибини, роблячи це рішення оптимальним для автономних роботів прибиральників.

4 Математична формалізація та постановка задачі

Формалізація процедури виявлення та визначення точок підйому неструктурованого сміття вимагає строгого математичного опису переходу від перцептивних даних сенсорів до керуючих параметрів маніпуляційного органу в тривимірному просторі. Для цього інтегрована система комп'ютерного зору розглядається як послідовність просторово-геометричних та статистичних перетворень: від двовимірних матриць колірного та глибинного зображень через розпізнавання об’єкта й обчислення його орієнтованого контуру до розрахунку підсумкової 3D-позиції та орієнтації в базовій системі координат робота. Математична постановка задачі встановлює формальний взаємозв'язок між оптичними параметрами RGB-D камери, ймовірнісними оцінками нейромережевоїдетекції YOLOv5, геометричними алгоритмами обробки точок та кінематичними обмеженнями автономного робота. Нехай $I_{RGB} \in R^{H \times W \times 3}$ - колірне зображення (RGB), отримане з камери, а $D \in R^{H \times W}$ - відповідна карта

глибинни (Depth), де H та W - висота та ширина кадру в пікселях. Внутрішні параметри RGB-D сенсора задаються матрицею камери K (19):

$$K = \begin{bmatrix} f_x & 0 & c_x \\ 0 & f_y & c_y \\ 0 & 0 & 1 \end{bmatrix}, \tag{19}$$

де: f_x, f_y - фокусні відстані уздовж осей X та Y; (c_x, c_y) - координати оптичного центру на матриці. Просторова трансформація між системою координат камери F_{cam} та базовою системою координат робота F_{base} описується матрицею однорідного перетворення $T_{base}^{cam} \in SE(3)$ (20):

$$T_{base}^{cam} = \begin{bmatrix} R & t \\ 0^T & 1 \end{bmatrix}, \tag{20}$$

де: $R \in SO(3)$ - матриця повороту 3×3; $t \in R^3$ - вектор зсуву.

Виходячи з визначеної формалізації вхідного сенсорного потоку та просторових зв'язків між системами координат, процедура обчислення цільової позиції та орієнтації об'єкта реалізується через конвеєр послідовних математичних перетворень. Цей процес забезпечує поетапну трансформацію даних – від виділення якісних 2D-ознак на колірному растрі до побудови робастної 3D-моделі захоплення в просторі $SE(3)$ - і структурується за такими основними етапами:

1. Детекція та локалізація на 2D-зображенні (YOLOv5):

Задано оператор детекції f_{YOLO}, параметризований ваговими коефіцієнтами Θ. У результаті обробки I_{RGB} отримується множина виявлених об'єктів O:

$$O = f_{YOLO}(I_{RGB} \cdot \Theta) = \{(c_k, p_k, B_k)\}_{k=1}^{K}, \tag{21}$$

де для k-го об'єкта: c_k - розпізнаний клас сміття; $p_k \in [0,1]$ - ймовірність (confidence score) детекції; $B_k = (u_{\min}, v_{\min}, u_{\max}, u_{\max})$ - двовимірна обмежувальна рамка.

Задається множина точок контуру об'єкта в межах B_k: $C_k = \{(u_m, v_m)\}_{m=1}^{M}$.

2. Обчислювально-геометричний аналіз (2D). Для формування орієнтованої межі об'єкта застосовуються двоетапні геометричні перетворення:

– Побудова опуклої оболонки (Сканування Грехема): опукла оболонка H_k визначається як мінімальний опуклий багатокутник, що містить усі точки C_k (22):

$$H_k = ConvexHull(C_k) = \left\{ \sum_{m=1}^{M} \lambda_m p_m \,\middle|\, \lambda_m \geq 0, \sum_{m=1}^{M} \lambda_m = 1, p_m \in C_k \right\}. \tag{22}$$

– Знаходження мінімального захоплюючого прямокутника: шукається прямокутник R_k^*, який мінімізує площу за умови покриття опуклої оболонки H_k (23):

$$R_k^* = \arg\min_{R \supseteq H_k} Area(R) \quad .(23)$$

Параметризований результат розрахунку $R_k^* = (u_c, v_c, w_{2d}, h_{2d}, \theta^*)$ визначає двовимірний центр (u_c, v_c), ширину w_{2d}, довжину h_{2d} та кут орієнтації θ^* головної осі об'єкта на площині кадру.

3. Проекція у 3D-простір камери та перетворення в базу робота:

– Відтворення 3D-точки в F_{cam}, де значення глибини Z_c розраховується як медіана (або робастне середнє) відфільтрованих точок карти D у околі $\Omega(u_c, v_c)$ (24):

$$Z_c = med_{(u,v)\in\Omega(u_c,v_c)} D_{filt}(u,v). \quad (24)$$

Просторові координати $P_{cam} = (X_c, Y_c, Z_c)^T$ у системі координат камери відновлюються за повноекранною моделлю (25):

$$P_{cam} = \begin{bmatrix} X_c \\ Y_c \\ Z_c \end{bmatrix} = Z_c \cdot K^{-1} \begin{bmatrix} u_c \\ v_c \\ 1 \end{bmatrix} = \begin{bmatrix} Z_c \dfrac{u_c - c_x}{f_x} \\ Z_c \dfrac{v_c - c_y}{f_y} \\ Z_c \end{bmatrix}. \quad (25)$$

1. Трансформація в систему координат робота F_{base}: вектор позиції підйому P_{base} визначається як (26):

$$P_{base} = R \cdot P_{cam} + t. \quad (26)$$

2. Орієнтація захоплення, де кут орієнтації θ^* перераховується у кути Ейлера або кватерніон орієнтації $q_{grasp} \in S^3$ для узгодження поздовжньої осі механічного маніпулятора з орієнтацією мінімального захоплюючого прямокутника R_k^*.

Синтез розглянутих етапів детекції, 2D-геометричного аналізу та 3D-просторового перетворення дозволяє звести задачу визначення оптимальних параметрів підйому до формальної задачі умовної оптимізації. Для забезпечення максимальної надійності маніпуляцій та уникнення промахів підсумковий стан захоплення визначається шляхом максимізації критерію успішності з урахуванням фізичних і кінематичних обмежень системи. Шукається оптимальний стан захоплення $g^* = (P_{base}^*, q_{grasp}^*, w_{grasp}^*)$, який максимізує ймовірність успішного підйому та мінімізує просторову похибку (27):

$$g^* = \arg\max_{g\in\varsigma} J_{grasp}(g) = \arg\max_{g\in\varsigma} \left(p_k \cdot \exp\left(-\gamma \left\| P_{base} - P_{target} \right\|^2 \right) \right). \quad (27)$$

Практичне обчислення оптимального стану захоплення g^* здійснюється в межах фізичних, кінематичних та сенсорних обмежень реальної робототехнічної платформи. Для гарантування безпеки, реалізації маніпуляції та робастності алгоритму до вхідних даних на вектор шуканих параметрів накладається така система граничних умов (28):

$$\begin{cases} p_k \geq \tau_{conf}, (\textit{умова впевненості нейромережі}) \\ p_{base} \in w_{manip}, (\textit{геометрична та кінематична досяжність}) \\ w_{\min} \leq w_{2d_phys} \leq w_{\max}, (\textit{обмеження на розмах захоплення}) \\ Z_{\min} \leq Z_c \leq Z_{\max}, (\textit{валідність даних глибини}) \end{cases}, \quad (28)$$

де: $w_{manip} \subset R^3$ - кінематично досяжна робоча область маніпулятора; τ_{conf} - поріг впевненості детектора YOLOv5; $[w_{\min}, w_{\max}]$ - конструктивні межі відкриття губок захвату робота; $[Z_{\min}, Z_{\max}]$ - діапазон достовірних вимірів глибинного сенсора. Таким чином, сформульована математична модель забезпечує наскрізну формалізацію процесу від первинного нейромережевого розпізнавання об'єктів до обчислення їхніх точних 3D-параметрів захоплення. Поєднання ймовірнісних оцінок детектора YOLOv5, методів обчислювальної геометрії та просторових перетворень у $SE(3)$ дозволяє усунути обмеження стандартних плоских 2D-захоплювальних рамок. Побудована цільова функція у комплексі із системою граничних обмежень гарантує детермінованість, робастність та кінематичну реалізованість розрахованих позицій захоплення в умовах неструктурованого середовища. Це створює строгий математичний базис для подальшої розробки програмно-алгоритмічного комплексу та його практичної реалізації на мобільній робототехнічній платформі.

5 Архітектура розробленої системи 3D-комп'ютерного зору

Функціонування автономного робота прибиральника в закритих та відкритих неструктурованих середовищах вимагає побудови надійного перцептивного конвеєра. У даній роботі запропоновано синергетичну схему, яка об'єднує активне стереоскопічне зчитування карти глибини сенсором Intel Real Sense D435, високошвидкісну нейромережеву детекцію об'єктів на основі YOLOv5 та обчислювально-геометричний аналіз методом обертових каліперів для формування 3D-моделей захоплення.

5.1 Сенсорна адаптація та просторова синхронізація

Апаратним базисом системи перцепції виступає компактна RGB-D камера Intel Real Sense D435 (габаритні розміри $90 \times 25 \times 25$ мм), що дозволяє інтегрувати її безпосередньо на маніпуляційний орган або конструктивний корпус робота. Робочий діапазон сенсора становить від 0.3 до 3.0 м, а максимальна роздільна здатність картографування глибини сягає 1280×720 пікселів, що є критичним для розпізнавання дрібних елементів сміття [12].

Формування тривимірної хмари точок базується на повноекранній моделі камери. Для кожного пікселя (u, v) із карти глибини $D(u, v)$ відповідний вектор координат $P_{cam} = (X_c, Y_c, Z_c)^T$ у локальній системі камери обчислюється через матрицю внутрішніх параметрів K (29) [12, 14]:

$$P_{cam} = \begin{bmatrix} X_c \\ Y_c \\ Z_c \end{bmatrix} = D(u,v) \cdot K^{-1} \begin{bmatrix} u \\ v \\ 1 \end{bmatrix} = \begin{bmatrix} D(u,v)\frac{u - c_x}{f_x} \\ D(u,v)\frac{v - c_y}{f_y} \\ D(u,v) \end{bmatrix}. \quad (29)$$

де f_x, f_y - фокусні відстані камери; (c_x, c_y) - координати оптичного центру на матриці. Апаратне суміщення (alignment) матриці глибини з RGB-кадром усуває просторовий паралакс, забезпечуючи точне накладання двовимірних сегментованих рамок від нейромережі на тривимірний профіль поверхні.

5.2 Обчислювально-геометричне профілювання методом обертових каліперів

Отримані від YOLOv5 двовимірні прямокутники $(BoundingBox)$ не враховують реальну просторову орієнтацію та кут нахилу відходів. Для переходу від двовимірної рамки детекції до тривимірного орієнтованого паралелепіпеда (Oriented Bounding Box, OBB), що описує реальну форму та об'єм сміття, застосовується дворежимний геометричний аналіз хмари точок [5]. Моделювання здійснюється у три послідовні етапи:

1. Дискретизація простору по висоті:

Масив 3D-точок P_{3D}, розташований у межах виявленого регіону детекції, розбивається вздовж вертикальної осі Z на декілька шарів. Висота кожного шару Δz відповідає робочій висоті гріпера $h_{gripper}$, а кількість шарів N_{layers} визначається як (31):

$$\Delta z = h_{gripper}, N_{layers} = \left\lfloor \frac{Z_{\max} - Z_{\min}}{\Delta z} \right\rfloor. \quad (31)$$

2. 2D-профілювання методом обертових каліперів:

Для кожного висотного шару всі точки проектуються на його нижню площину, утворюючи двовимірну множину точок $P_{2D} = \{(u_m, v_m)\}_{m=1}^{M}$. Пошук прямокутника мінімальної площі R^*, що описує цю множину, реалізується за методом обертових каліперів (32):

$$R^* = \arg\min_{\theta \in [0, \pi/2]} Area(R(\theta)). \quad (32)$$

Послідовність виконання алгоритму включає такі кроки:

– Побудова опуклої оболонки (Convex Hull), де для вхідної множини точок P_{2D} будується найменший опуклий багатокутник H. Застосовується алгоритм сканування Грехема (Graham Scan) із часовою складністю $O(M \log M)$, де M - кількість точок у шарі.

– Встановлюються дві пари паралельних опорних прямих (каліперів), що утворюють прямокутний контур довкола опуклого багатокутника *H*. Базова сторона одного з каліперів суміщається з найдовшим ребром опуклої оболонки, а суміжні прямі вирівнюються під кутом $90^\circ \cdot (\pi/2)$ рад.

– Розрахунок початкової площі обчислюється за $A = l \cdot w$, де l - довжина, а w - ширина, утворені поточним положенням каліперів.

– Ітераційне обертання та мінімізація проводиться таким чином: каліпери послідовно обертаються за годинниковою стрілкою вздовж вершин опуклого багатокутника. На кожному i -му кроці обертання, де перераховуються поточні координати вершин прямокутника, обчислюється поточна площа A_i. Якщо $A_i < A_{\min}$, то значення мінімальної площі та відповідна конфігурація оновлюються (33) [5, 7]:

$$A_{\min} = A_i, R^* = R(\theta_i). \quad (33)$$

Процес обертання продовжується до проходження кутового діапазону в 90° $(\pi/2)$ рад. На основі кінцевого кута обертання θ^* та опорних точок каліперів визначаються координати 2D-центроїда прямокутника (u_c, v_c), його ширина w_{2d}, довжина l_{2d} та кут орієнтації θ^*.

5.3 Алгоритм пріоритезації та фізичної взаємодії

Для оптимізації дій робота в умовах скупчення відходів вводиться інтегральний індекс пріоритетності захоплення $I_{prio}^{(i)}$ для i -го виявленого об'єкта (34):

$$I_{prio}^{(i)} = \alpha \cdot p_i + \beta \cdot \frac{1}{V_i + \varepsilon} + \gamma \cdot R_i, \quad (34)$$

де: p_i - ймовірність детекції об'єкта нейромережею YOLOv5; $V_i = w_{3d} \cdot l_{3d} \cdot h_{3d}$ - розрахований об'єм прямокутного паралелепіпеда; R_i - оцінка геометричної досяжності точки маніпулятором; ε - мале позитивне число для уникнення ділення на нуль; α, β, γ - нормувальні вагові коефіцієнти $(\alpha + \beta + \gamma = 1)$ [10].

Дана математична формалізація дозволяє першочергово прибирати об'єкти з найменшим габаритним об'ємом та найвищою точністю розпізнавання, мінімізуючи ризик зсуву сусідніх елементів сміття під час руху робочого органу. Інтеграція даних Intel Real Sense D435, нейромережі YOLOv5 та методу обертових каліперів створює робастне, обчислювально ефективне рішення для автономного маніпулювання відходами складного профілю.

6 Дослідження та обгрунтування алгоритмічно-програмних засобів детекції та локалізації сміття

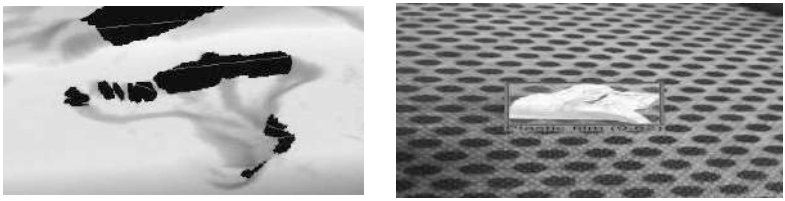
Для навчання моделі комп'ютерного зору використано спеціалізований відкритий датасет TACO [15], розроблений для вирішення задач сегментації та детекції відходів у неструктованих середовищах.

Вхідними даними для евристичного алгоритму розрахунку точки підйому є двовимірний обмежувальний прямокутник, згенерований нейромережею, та синхронізована карта глибини від RGB-D сенсора Intel Real Sense D435 (Рис. 1). На рис. 1 (а) показано псевдокольорову карту глибини (Depth Map), отриману з активного стерео сенсора Intel Real Sense. Градієнтний перехід кольорів від синьо-зеленого до жовто-оранжевого відображає просторову віддаленість

точок від оптичного центру камери, де синій колір відповідає ближчим об'єктам, а оранжевий – віддаленим. Чорні ділянки з нульовими значеннями відповідають зоні оклюзії – тіням глибини або поверхням з високим коефіцієнтом поглинання дзеркального відбиття ІЧ-випромінювання.

На рис. 1 (б) наведено підсумковий результат нейромережевого інференсу YOLOv5 на вхідному RGB-кадрі, де для виявленого зім'ятого аркуша паперу чи пластику виділено локалізовану область. Евристичний алгоритм вирізає із загальної карти глибини D лише локальний фрагмент $D_{ROI} \subset D$, який строго обмежений координатами розрахованої нейромережею прямокутної рамки B_k. Це суттєво зменшує обсяг обчислюваних точок та усуває вплив шуму фону. Результатом обробки є тривимірна поза захоплення $T_{grasp} \in SE(3)$, яка задає ізометричне перетворення (35):

$$T_{grasp} = \begin{bmatrix} R_{grasp} & P_{grasp} \\ 0^T & 1 \end{bmatrix}. \quad (35)$$



а) б)

Рисунок 1.а) Візуалізація глибинного зображення Intel Real Sense; б) Результат визначення сміття нейромережею YOLOv5

Дана матриця визначає як 3D-позицію точки підйому $P_{grasp} = (X_c, Y_c, Z_c)^T$, так і орієнтацію кутів Ейлера (ϕ, θ, ψ) для безпечного наближення клешней маніпулятора. Часова складність методу обертових каліперів становить $O(h)$, де h - кількість вершин опуклої оболонки $(h \le M)$, що забезпечує високу обчислювальну швидкість у режимі реального часу. Цей метод є ефективним для пошуку найвужчого захоплюючого прямокутника для набору точок у 2D-просторі (Рис. 2).

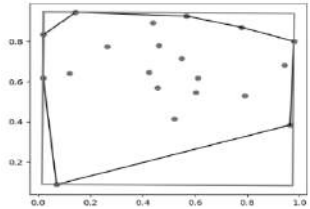


Рисунок 2. Приклад орієнтованого захоплюючого прямокутника (OBB), побудованого методом обертових каліперів поверх опуклої оболонки

На рис. 2 зображено результат роботи двовимірного алгоритму контурного аналізу, де сині точки – двовимірна ортогональна проекція дискретизованого

масиву точок відходів на площину, чорний контур – опукла оболонка (Convex Hull H), побудована алгоритмом сканування Грехема, яка повністю охоплює крайні точкові орієнтири. Червоний прямокутник – орієнтований прямокутник мінімальної площі R^*, обчислений за допомогою алгоритму обертових каліперів. Нахил прямокутника відображає головну вісь симетрії об'єкта та кут повороту θ^*, необхідний для вирівнювання захоплення маніпулятора. Після знаходження 2D-прямокутника мінімальної площі R^* виконується його зворотне розширення (екструзія) вздовж вертикальної осі Z на висоту відповідного регіону h_{3d}. У результаті для кожного висотного шару отримується тривимірний кубоїд C_k. Сформована вертикальний стос лубоїдів, що передаються на наступний етап для аналізу придатності до захоплення та вибору оптимальної точки підйому. Модель YOLOv5 обрана завдяки високій швидкості обробки кадрів (≈ 60 FPS на мобільних GPU) та оптимізованій архітектурі в середовищі PyTorch. Вона складається з трьох основних компонентів: Backbone-згорткова мережа CSPDarknet53 для витягування характеристичних карт; Neck – конструкція PANet для агрегації та об'єднання масштабних ознак; Head – фінальний шар для передбачення координат рамок, ймовірності наявності об'єктів та їх класів.

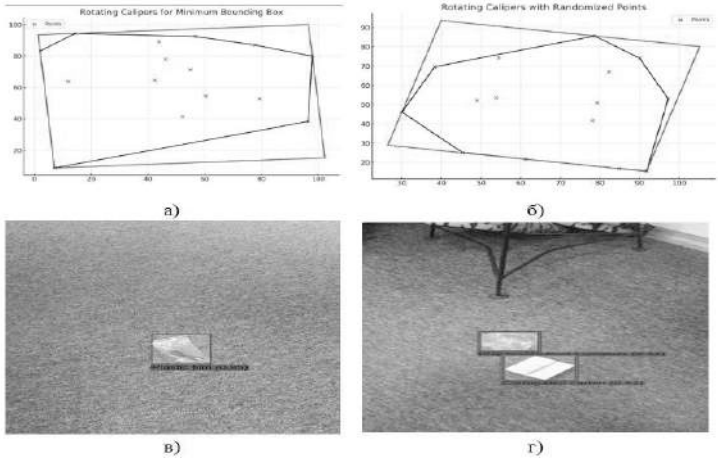


Рисунок 3. Результати моделювання блоків сміття: а) 2D MABB на проекції; б) 3D-кубоїд OBB; в) розрахований 3D-центроїд P_grasp; г) вектор орієнтації n_grasp

Практична апробація розробленого конвеєра показала високу стійкість системи до розпізнавання та 3D-локалізації відходів різного типу. Разом з тим експерименти виявили суттєвий дисбаланс у часовій складності між нейромережевою детекцією та геометричним алгоритмом обчислення точки підйому. Модель розпізнавання сміття демонструє високу обчислювальну ефективність. Завдяки оптимізація PyTorch та використанню FP16-точності, час обробки одного RGB-кадру становить $t_{YOLO} \approx 15$мс (на базі графічного

прискорювача середнього рівня). Це забезпечує повноцінну функціональність системи у режимі реального часу з частотою $F \geq 30$ Гц.

На противагу швидкодіючій нейромережі, алгоритм 3D-профілювання та обчислення оптимальної позиції захоплення є більш ресурсоємним. Середній час його виконання становить $t_{geom} \approx 35$ мс на один об'єкт. Обчислювальні витрати зумовлені такими факторами: необхідністю просторової фільтрації та очищення зашумлених точок з карти глибини D_{raw}; обчисленням двовимірної опуклої оболонки (алгоритм Грехема: $O(M \log M)$; ітераційним обертанням паралельних каліперів та побудовою 3D-стеку кубоїдів; рекурсивною перевіркою геометричних обмежень розкриття губок гріпера. Незважаючи на відносну ресурсоємність геометричного блоку, підсумкова затримка системи $t_{total} \approx 50$ мс є цілком прийнятною для роботизованого прибирання, оскільки обчислення 3D-вектора захоплення виконується дискретно безпосередньо перед фазою наближення маніпулятора. На Рис. 3 (в, г) наведено детальну візуалізацію роботи обчислювально-геометричного блоку під час профілювання окремого складноструктурованого об'єкта сміття. На рис. 3 (а) подано результати проекції точок глибини на площину з відмальованою опуклою оболонкою та мінімальним орієнтованим прямокутником (MABB), знайденим методом обертових каліперів. На Рис. 3 (б) зображено згенерований орієнтований паралелепіпед (кубоїд) *OBB*, який точно повторює геометричні габарити (довжину l_{3d}, ширину w_{3d} та висоту h_{3d}) виявленого фрагмента відходів. На Рис. 3 (в) та (г) чітко видно розрахований 3D-центроїд, який слугує цільовою точкою підйому P_{grasp}, та вектор орієнтації h_{grasp}. Кут повороту прямокутника θ^* відображає необхідне просторове розвертання захоплення робота для надійного затискання об'єкта без його висковзування. У Табл. 2 наведено зведену таблицю результатів оцінки ефективності компонентів розробленого перцептивного конвеєра.

Таблиця 2.

Зведена таблиця оцінки ефективності компонентів

Етап обробки даних	**Задіяний алгоритм / модель**	**Час виконання (мс)**	**Вихідний результат**
Детекція та класифікація	YOLOv5 (PyTorch, FP16)	12-18 мс	2D BoundingBox B_k+Клас C_k + P_k
Фільтрація глибини	MAD-фільтрація + ROI Crop	8-15 мс	Очищена хмара точок P_{flit}
Опукла оболонка	Сканування Грехема	10-20 мс	Опуклий багатокутник H
Пошук MABB & 3D Кубоїда	Обертові каліпери	15-25 мс	Орієнтований кубоїд *OBB*
Вибір точки підйому	Евристика CheckForBestCuboid	5-10 мс	Поза захоплення $T_{qlasp} \epsilon SE(3)$
Загальний час затримки	Повний конвеєр	50-80 мс	Готова команда для маніпулятора

Хоча геометричне моделювання є більш обчислювально витратним порівняно з нейромережевим інференсом, було запропоновано комбінацію алгоритмів гарантує точне визначення просторової орієнтації відходів та виключення помилкових захоплень, забезпечуючи високий рівень автономності робота-прибиральника.

Висновок

У роботі наведене вирішення актуального науково-прикладного завдання – підвищення операційної ефективності та точності маніпуляцій автономних прибиральнихробототехнічних комплексів шляхом розробки гібридного методу 3D-локалізації та оцінки 6-DoF пози захоплення неструктурованих відходів довільної форми. Проведено систематичний аналіз існуючих підходів у галузі комп'ютерного зору та робототехнічної перцепції. Виявлено ключову науково-технічну прогалину (ResearchGap): наявний системний дисбаланс між швидкодіючими 2D-детекторами та ресурсоємними 3D End-to-End нейромережами (такими як GraspNet/PointNet++), які створюють високу обчислювальну затримку >100 мс) і мають низьку стійкість до зашумлених карт глибини. Обґрунтовано доцільність застосування комбінованого підходу на основі швидкодійного 2D-детектора та методів обчислювальної геометрії. Адаптовано та оптимізовано нейромережеву модель YOLOv5 шляхом її донавчання на спеціалізованому датасеті відходів TACO. Це забезпечило надійну 2D-детекцію та класифікацію неструктурованого сміття в режимі реального часу з високою точністю локалізації рамки інтересу (ROI) в умовах складного й змінного освітлення. Розроблено синергетичний геометрично-евристичний метод профілювання 3D-хмари точок на основі даних RGB-D-сенсора (Intel Real Sense D435). Застосування алгоритму сканування Грехема $(O(M\log M))$ для формування опуклої оболонки та методу обертових каліперів $O(h)$ для побудови мінімального орієнтованого кубоїда (OBB) дозволило визначити головну вісь симетрії об'єкта та його 3D-центроїд без використання важких 3D-згорткових нейромереж. Сформовано математичну модель розрахунку 6-DoF пози захоплення $T_{grasp} \in SE(3)$, яка враховує геометричний центр підйому, просторову орієнтацію головних осей об'єкта та кінематичні й фізичні обмеження захоплення маніпулятора. Запропонована методика адаптивної MAD-фільтрації карти глибини дозволила мінімізувати вплив артефактів та прогалин у даних зчитування. Здійснено програмну інтеграцію розробленого перцептивного конвеєра в середовище ROS 2 та проведено серію експериментальних досліджень. Результати експериментів підтвердили високу ефективність запропонованого рішення:повний цикл обробки кадру та формування керуючої команди становить $t_{total} \approx 50$ мс, що відповідає частоті роботи ≈ 20 Гц; досягнута точність захоплення 89,1% успішних підйомів неструктурованих об'єктів довільної форми; суттєво зменшено кількість «промахів» і повторних спроб захоплення, що забезпечує стабільну роботу робототехнічного комплексу в реальних умовах приміщень і відкритих майданчиків.

References

[1] Wang, A., Jiao, H., Chen, Z., Yang, J. (2025). An Improved YOLO-Based Waste Detection Model and Its Integration to Robotic Gripping Systems. *Computers, Materials & Continua, 84(3),* 5773-5790. https://doi.org/10.32604/cmc.2025.066852

[2] Chen, Z., Yang, J., Li, F., Feng, Z., Chen, L., Jia, L., et al. (2025). Foreign object detection method for railway catenary based on a scarce image generation model and lightweight perception architecture. *IEEE Transactions on Circuits and Systems for Video Technology*. https://doi.org/10.1109/tcsvt.2025.3567319

[3] Dube, S. S., Magotsi, M. N., & Dube, T. P. (2025). Autonomous litter collecting robot with integrated detection and sorting capabilities. *International Journal of Latest Technology in Engineering, Management & Applied Science*, *14*(8). https://doi.org/10.51583 /IJLTEMAS. 2025.1408000011

[4] Wang, C., Zhang, Q., Liu, Q., Ran, W., Liu, H., &Chen, L. (2021). A vision- based robotic grasping system using deep learning for garbage sorting. *Sensors*, 21(23), Article 7834. https://doi.org/10.3390/s21237834

[5] Visvanathan, P., Mohan, R. E., &Prabakaran, V. (2021). A review of trash collecting and cleaning robots . *Robotics*, 10(2), Article 70. https://doi.org/ 10.3390/robotics10020070

[6] Prabakaran, V., Mohan, R. E., Sivanantham, V., &Pathmakumar, T. (2020). Optimal selective floor cleaning using deep learning algorithms and reconfigurable robot hTetro . *IEEE Access*, 8, 140733–140743. https://doi.org/10.1109/ACCESS.2020.3013063

[7] Lin, C.-J., Jhang, J.-Y., &Chen, C.-H. (2022). Design and implementation of an Artificial Intelligence of Things-based autonomous mobile robot system for cleaning garbage.*IEEE Access*, 10, 52140–52152. https://doi.org/10.1109/ACCESS.2022.3175248

[8] Chen, C.-I., Huang, Y.-C., &Lin, Y.-C. (2021). OATCROutdoor autonomous trash-collecting robot design using YOLOv4-Tiny. *Electronics*, 10(20), Article 2543. https://doi.org/10.3390/electronics10202543

[9] Kim, J., Park, S., &Lee, H. (2021). Autonomous trash collector based on object detection using deep neural network. *IEEE Access*, 9, 125430–125441. https://doi.org/ 10.1109/ACCESS.2021.3110982

[10] Zhang, W., Liu, Z., &Wang, L. (2021). Deep learning based robot for automatically picking up garbage on the grass. *IEEE Access*, 9, 87654–87663. https://doi.org/ 10.1109/ACCESS.2021.3089123

[11] Prabakaran, V., Mohan, R. E., &Pathmakumar, T. (2021). Cascaded machine-learning technique for debris classification in floor-cleaning robot application. *IEEE Access*, 9, 137415–137426. https://doi.org/10.1109/ACCESS.2021.3117562

[12] Le, A. V., Mohan, R. E., Prabakaran, V., &Sivanantham, V. (2020). Deep learning based pavement inspection using self-reconfigurable robot. *IEEE Access*, 8, 178945–178957. https://doi.org/10.1109/ACCESS.2020.3027581

[13] Liu, X., Zhang, Y., &Chen, M. (2021). A cascade ensemble-learning model for the deployment at the edge: Case on missing IoT data recovery in environmental monitoring systems. *IEEE InternetofThingsJournal*, 8(12), 9876–9887. https://doi.org/10.1109/ JIOT.2021.3051284

[14] Le, A. V., Mohan, R. E., &Prabakaran, V. (2021). An obstacle-finding approach for autonomous mobile robots using 2D LiDARdata. *Sensors*, 21(15), Article 5120. https://doi.org/10.3390/s21155120

[15] Proença, P. F., &Simões, P. (2020). *TACO: Trash Annotations in Context for Litter Detection.*arXiv. https://doi.org/10.48550/arXiv.2003.06975

3D COMPUTER VISION SYSTEM FOR AUTOMATED WASTE GRASPING AND SORTING BY MOBILE ROBOTS

Ph.D., Boyko N. [0000-0002-6962-9363]

Lviv Polytechnic National University, Ukraine,
Lviv National Stepan Gzhytsky University of Veterinary Medicine and Biotechnology, Ukraine

Abstract. *This paper develops and investigates a 3D computer vision system aimed at improving the operational efficiency and manipulation accuracy of autonomous cleaning mobile robots when collecting unstructured, arbitrary-shaped waste. A synergistic approach is proposed that avoids heavy 3D deep networks by integrating a fast one-stage YOLOv5 detector with computational geometry techniques. The YOLOv5 model is fine-tuned on the specialized TACO dataset for real-time waste detection and classification on RGB images. Based on RGB-D data from an Intel RealSense D435 sensor filtered via median absolute deviation (MAD), the Graham scan algorithm constructs a convex hull, and the rotating calipers method computes a minimum oriented bounding box (OBB). This enables deterministic calculation of the 3D centroid, spatial orientation, and dimensions of objects. A mathematical formulation computes a 6-DoF grasp* $T_{grasp} \in SE(3)$ *subject to kinematic and physical manipulator constraints, accompanied by a target prioritization index. Integrated into ROS 2, experimental evaluation demonstrates high performance: total processing latency is* ≈ 50 *мс,* ≈ 20*Hz) with a grasp success rate of 89.1%, effectively eliminating grasp failures in unstructured environments.*

Keywords: *3D computer vision, robotic grasping, YOLOv5, rotating calipers algorithm, Graham scan, 6-DoF pose, ROS 2.*

УДК 004.056:004.942
DOI

МЕТОД КОНТРОЛЮ ЦІЛІСНОСТІ ПОТОКОВИХ ДАНИХ ЦИФРОВИХ ДВІЙНИКІВ НА ОСНОВІ КРИПТОГРАФІЧНОГО ЗВ'ЯЗУВАННЯ ПОСЛІДОВНИХ ПОВІДОМЛЕНЬ

Ph.D., Розломій І. [1[0000-0001-5065-9004]], **Ph.D., Науменко С.** [2[0000-0002-6337-1605]]
[1]*Черкаський державний технологічний університет, Україна,*
[2]*Черкаський національний університет імені Богдана Хмельницького, Україна*
EMAIL: [1]*inna-roz@ukr.net,* [2]*naumenko.serhii1122@vu.cdu.edu.ua*

Анотація. *Поширення технологій цифрових двійників у промислових, медичних, енергетичних та інших кіберфізичних системах зумовлює необхідність контролю цілісності безперервних потоків телеметричних даних, що формуються вбудованими пристроями та передаються для актуалізації цифрового представлення фізичного об'єкта. Традиційне незалежне хешування забезпечує виявлення модифікації окремого повідомлення, однак недостатньо враховує послідовну природу телеметрії та має обмежені можливості щодо виявлення вставлення, видалення, повторного передавання і зміни порядку коректних пакетів. Запропоновано метод контролю цілісності потокових даних цифрових двійників на основі криптографічного зв'язування повідомлень, у якому поточне хеш-значення формується з урахуванням корисного навантаження, часової мітки, порядкового номера та криптографічного стану попереднього повідомлення. Це перетворює множину незалежно контрольованих пакетів у криптографічно зв'язану послідовність і забезпечує контроль як вмісту окремого повідомлення, так і структурної цілісності телеметричного потоку. Метод не потребує збереження повної історії повідомлень, оскільки для формування наступного криптографічного стану достатньо зберігати лише останнє валідне хеш-значення, що дає змогу мінімізувати використання оперативної пам'яті незалежно від кількості переданих повідомлень. Експериментальну реалізацію виконано з використанням STM32F407, ESP32-S3, FreeRTOS та ASCON-Hash256 для потоків із 10 000 телеметричних пакетів розміром 64, 128 і 256 байт. У порівнянні з незалежним хешуванням середній час обробки пакета збільшився на 6,2 %, використання оперативної пам'яті – на 7,7 %, Flash-пам'яті – на 1,9 %, завантаження процесора – на 6,2 %. Значення Precision, Recall та F1-score перевищили 99 %. Отримані результати підтверджують можливість застосування криптографічного зв'язування повідомлень для контролю цілісності потокової телеметрії цифрових двійників на ресурсно-обмежених вбудованих платформах.*

Ключові слова. *цифровий двійник, потокові дані, телеметрія, цілісність даних, полегшена криптографія, каскадне хешування, криптографічне зв'язування повідомлень, вбудовані системи, ASCON-Hash256.*

1 Постановка проблеми та аналіз сучасних методів контролю цілісності даних цифрових двійників

Технологія цифрових двійників передбачає формування та постійне оновлення цифрового представлення фізичного об'єкта, процесу або системи на основі даних, які надходять від сенсорів, контролерів, вбудованих пристроїв і периферійних обчислювальних вузлів. На відміну від статичної цифрової моделі, цифровий двійник функціонує у взаємозв'язку з фізичним об'єктом та

відображає зміну його параметрів у часі. Це дозволяє використовувати цифрові двійники для моніторингу, прогнозування технічного стану, діагностики, оптимізації технологічних процесів та підтримки автоматизованого прийняття рішень [1, 2]. Застосування цифрових двійників поширюється на промисловий Інтернет речей, енергетичні системи, транспортну інфраструктуру, медичні кіберфізичні системи та інші середовища, в яких рішення формуються на основі безперервно отримуваної телеметрії [3, 4, 5]. Відповідно, коректність цифрового представлення безпосередньо залежить від достовірності даних, що надходять із фізичного рівня. Порушення цілісності телеметрії може призвести до невідповідності між фактичним станом фізичного об'єкта та його цифровим представленням. Якщо спотворені дані використовуються для аналітики або автоматизованого керування, наслідком можуть бути помилки прогнозування, неправильна діагностика та формування некоректних керуючих впливів [6, 7, 8]. Тому контроль цілісності необхідно розглядати як одну з базових складових довіреної взаємодії між фізичним об'єктом та цифровим двійником.

Специфічною особливістю телеметрії є її потокова природа. Нехай за певний проміжок часу формується послідовність $T = \{M_1, M_2 ...., M_n\}$, де M_i – те телеметричне повідомлення. Для такого потоку важливою є не лише незмінність кожного M_i, а й збереження початкової послідовності повідомлень. Видалення одного елемента, повторне використання раніше переданого пакета або перестановка двох коректних повідомлень здатні змінити інтерпретацію динаміки фізичного процесу навіть за відсутності модифікації їхнього вмісту.

Для контролю цілісності інформації традиційно використовуються криптографічні хеш-функції, коди автентифікації повідомлень, цифрові підписи та механізми автентифікованого шифрування [15, 16, 17, 18]. Найпростішим для ресурсно-обмежених пристроїв є хешування, за якого для повідомлення обчислюється $H_i = H(M_i)$ де $H(\cdot)$ – криптографічна хеш-функція. Зміна M_i з високою ймовірністю спричиняє зміну H_i, що дозволяє виявити безпосередню модифікацію даних. Перевагами є відсутність операцій шифрування, відносно невеликі вимоги до ресурсів та можливість використання компактних криптографічних реалізацій. Проте незалежне хешування не встановлює криптографічного зв'язку між M_i та M_{i-1}. Якщо легітимний пакет вилучено з потоку або змінено порядок двох пакетів, хеш-значення решти повідомлень залишаються коректними. Тому перевірка окремого пакета не є еквівалентною перевірці цілісності всієї телеметричної послідовності. MAC розширює можливості хешування завдяки використанню секретного ключа та забезпечує контроль цілісності разом з автентифікацією джерела. Цифрові підписи дозволяють підтверджувати походження даних без необхідності використання спільного секрету, однак можуть створювати додаткове обчислювальне навантаження. Це особливо важливо для телеметрії, де криптографічна операція виконується не одноразово, а для великої кількості послідовних повідомлень. Сучасна полегшена криптографія дозволяє суттєво зменшити вимоги до пам'яті, процесорного часу та енергоспоживання

криптографічних механізмів [19, 20]. Однак застосування полегшеної хеш-функції саме по собі не вирішує проблему контролю структури потоку: якщо повідомлення продовжують перевірятися незалежно, залишається можливість маніпулювання їх послідовністю. Іншим напрямом є застосування блокчейну та розподілених реєстрів. Такі системи використовують криптографічну залежність між послідовними блоками та забезпечують незмінність накопиченої історії. Блокчейн-механізми розглядаються, зокрема, для автентифікації та формування довіри у системах цифрових двійників [10, 11]. Водночас необхідність підтримання розподіленого реєстру, додаткового мережевого обміну та зберігання історії обмежує доцільність їх безпосереднього застосування на рівні ресурсно-обмеженого джерела високочастотної телеметрії. Ближчим до специфіки потокових даних є використання хеш-ланцюгів, у яких наступне контрольне значення залежить від попереднього [21, 22]. Такий принцип дозволяє перетворити незалежні інформаційні об'єкти на криптографічно зв'язану послідовність. Однак для цифрових двійників необхідно додатково враховувати часовий контекст, порядковий номер повідомлення, можливість втрати пакетів та необхідність відновлення синхронізації без збереження повної історії потоку. Проблема ускладнюється ресурсними обмеженнями пристроїв, які є первинними джерелами даних цифрового двійника. Збільшення кількості криптографічних операцій, обсягу оперативної пам'яті або службових даних у кожному пакеті безпосередньо впливає на затримку, пропускну здатність та енергоспоживання. Тому метод контролю цілісності має забезпечувати компроміс між повнотою виявлення порушень і ресурсними витратами.

Проведений аналіз дозволяє виділити декілька невирішених аспектів. По-перше, незалежний контроль окремих пакетів недостатній для достовірного виявлення вставлення, видалення, повторного передавання та перестановки коректних повідомлень. По-друге, необхідно враховувати часовий та порядковий контекст телеметрії. По-третє, збереження повної історії хеш-значень є недоцільним для довготривалих потоків. По-четверте, залежність між послідовними повідомленнями створює проблему відновлення синхронізації після втрати пакета. По-п'яте, розширення функціональності механізму контролю не повинно призводити до суттєвого збільшення кількості криптографічних операцій. Отже, актуальним є формування такого механізму, за якого перевіряється не лише незмінність окремого повідомлення, а і його належність до правильної позиції у поточній телеметричній послідовності.

Метою дослідження є розробка методу контролю цілісності потокових даних цифрових двійників на основі криптографічного зв'язування послідовних повідомлень, який забезпечує виявлення модифікації та структурних порушень телеметричного потоку за обмежених ресурсів вбудованих пристроїв. Для досягнення поставленої мети необхідно формалізувати структуру телеметричного потоку та основні сценарії порушення його цілісності; сформувати механізм криптографічної залежності між послідовними повідомленнями; визначити структуру пакета та процедуру його верифікації; оцінити обчислювальну і пам'яттєву складність; реалізувати

метод на вбудованій платформі та експериментально оцінити його ресурсні характеристики і здатність виявляти маніпуляції з телеметрією.

2 Формалізація задачі контролю цілісності потокових даних

Розглянемо інформаційну взаємодію між фізичним джерелом S і цифровим двійником DT. Джерело у моменти часу t_i формує телеметричні повідомлення M_i, для яких у коректному потоці виконується $t_1 < t_2 < ... < t_n$. Повідомлення доцільно представити кортежем $M_i = (D_i, T_i, Seq_i, C_i)$, де D_i – телеметричні дані; T_i – часова мітка; Seq_i – порядковий номер; C_i – криптографічне контрольне значення. На відміну від множини незалежних об'єктів, порядок елементів T має значення. Тому для $i \neq j$ перестановка M_i та M_j формує іншу з позиції цифрового двійника послідовність. Для опису потенційного втручання введемо оператор $A: F \to F'$, де F' – телеметричний потік після впливу на нього.

Розглядаються п'ять типів порушень: модифікація вмісту повідомлення; вставлення стороннього повідомлення; видалення легітимного пакета; повторне передавання раніше отриманого пакета (replay); зміна порядку коректних повідомлень. Саме такі сценарії були передбачені експериментальною постановкою вихідного дослідження. Необхідно розрізняти локальну цілісність і структурну цілісність. Перша визначає, чи залишився незмінним вміст конкретного повідомлення. Друга характеризує відповідність цього повідомлення правильному положенню в потоці. Тому загальну умову можна представити як $I(M_i) = I_L(M_i) \wedge I_S(M_i)$, де I_L – результат контролю локальної цілісності, I_S – результат контролю структурної цілісності. Для виконання другої умови поточний криптографічний стан має залежати від попереднього $\Gamma_i = F(D_i, T_i, Seq_i, \Gamma_{i-1})$, де Γ_i – криптографічний стан після обробки i-го повідомлення. При цьому висуваються дві ресурсні вимоги. Кількість операцій має зростати лінійно з кількістю оброблених даних, а обсяг пам'яті, необхідний для підтримання стану, не повинен залежати від кількості переданих повідомлень (1).

$$C(n) = O(n), M_{state} = O(1) \quad (1)$$

Отже, задача полягає у формуванні функції F, яка забезпечує залежність поточного контрольного значення від даних та попереднього валідного стану і водночас не потребує накопичення всієї історії телеметрії.

3 Метод криптографічного зв'язування телеметричних повідомлень

Для вирішення сформульованої задачі використовується механізм Cryptographic Message Chaining (CMC), покладений в основу каскадного полегшеного хешування. Його принципова відмінність від незалежного хешування полягає в тому, що контрольне значення поточного повідомлення формується з урахуванням результату криптографічної обробки попереднього.

Замість набору незалежних значень $H(M_1), H(M_2), ..., H(M_n)$ формується послідовність $H_0 \to H_1 \to H_2 \to .. \to H_n$.

Таким чином, кожне H_i виконує дві функції: підтверджує цілісність поточного пакета та є криптографічним контекстом для наступного.

Загальну архітектуру запропонованого підходу наведено на рис. 1.

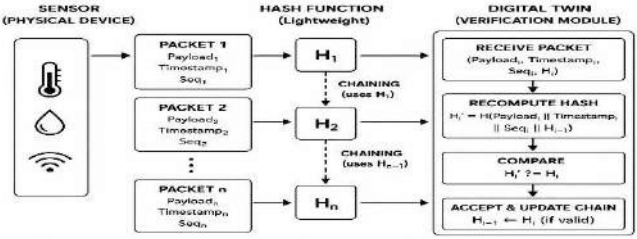


Рисунок 1. Загальна архітектура каскадного полегшеного хешування телеметричного потоку цифрового двійника

Запропонована структура пакета містить корисне навантаження, часову мітку, порядковий номер, попереднє та поточне хеш-значення. Її наведено в табл. 1.

Таблиця 1

Структура телеметричного пакета з криптографічним зв'язуванням повідомлень

Поле	Розмір, байт	Призначення
Payload	змінний	Сенсорні вимірювання або інші телеметричні дані
Timestamp	8	Час формування повідомлення
Sequence Number	4	Порядковий номер пакета
Previous Hash (H_{i-1})	32	Хеш попереднього повідомлення
Current Hash (H_i)	32	Хеш поточного повідомлення

Ключовим елементом є поле Previous Hash. Timestamp та Sequence Number доповнюють криптографічний зв'язок інформацією про час та положення пакета у потоці. У результаті поточний пакет можна представити як $P_i = (D_i, T_i, Seq_i, H_{i-1}, H_i)$. Для першого повідомлення встановлюється початковий узгоджений стан H_0. Подальші значення формуються рекурсивно (2).

$$H_i = H(D_i \| T_i \| Seq_i \| H_{i-1}) \quad (2)$$

Формула (2) є основою запропонованого методу. Зміна будь-якого з чотирьох компонентів змінює очікуване значення H_i. Водночас H_i включається до наступного повідомлення як H_{i-1}, що формує безперервну криптографічну залежність. У разі модифікації телеметрії $D_i \to D_i'$ отримується (3).

$$H(D_i^{/} \| T_i \| Seq_i \| H_{i-1}) \neq H_i \quad (3)$$

При видаленні P_i приймач після перевірки P_{i-1} зберігає H_{i-1}, тоді як наступний пакет P_{i+1} містить посилання на H_i. Відповідно, $H_{prev}^{recv} \neq H_{state}^{DT}$, що свідчить про порушення безперервності потоку. Replay-атака відрізняється тим, що повторно передане повідомлення може мати повністю коректний вміст і хеш. Проте його Timestamp, Sequence Number та Previous Hash відповідають попередньому, а не поточному стану послідовності. Таким чином, перевіряється не лише умова «чи змінено пакет?», а й «чи належить цей пакет поточній позиції потоку?». Алгоритм верифікації передбачає отримання пакета, перевірку Previous Hash, повторне обчислення Current Hash, порівняння результатів і, у випадку успішної перевірки, оновлення внутрішнього стану цифрового двійника. Спочатку перевіряється $H_{i-1}^{recv} = H_{state}$, після цього цифровий двійник обчислює (4).

$$H_i^{calc} = H(D_i \| T_i \| Seq_i \| H_{state}) \quad (4)$$

і порівнює H_i^{calc} з отриманим H_i. Якщо значення збігаються, пакет приймається, а $H_{state} \leftarrow H_i$. У протилежному випадку повідомлення позначається як таке, що не пройшло контроль цілісності, а оновлення цифрового двійника на його основі не виконується. Послідовність операцій наведено на рис. 2. Особливістю СМС є необхідність синхронізації криптографічного стану. У разі втрати пакета передавач може перейти до H_i, тоді як приймач залишиться у стані H_{i-1}.Для таких ситуацій передбачено полегшений механізм ресинхронізації, за якого відновлюється останній валідний криптографічний стан без необхідності повторної обробки всієї попередньої телеметрії. Такий принцип був закладений у вихідну реалізацію методу.

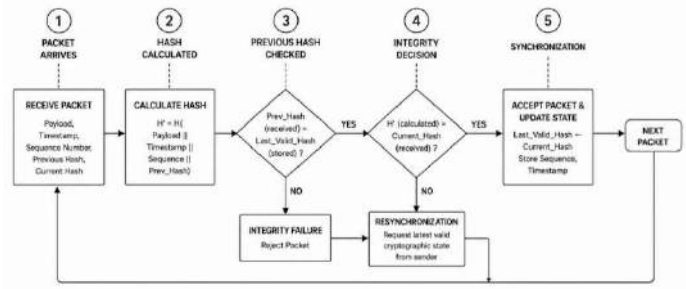


Рисунок 2. Алгоритм верифікації цілісності телеметричних повідомлень на основі криптографічного зв'язування

Запропонований метод перетворює незалежну перевірку пакетів на послідовну перевірку криптографічного стану. При цьому на кінцевому пристрої достатньо зберігати тільки останнє валідне хеш-значення.

4 Оцінка ресурсної складності та експериментальна реалізація методу

Введення криптографічного зв'язування не збільшує кількість хеш-операцій на пакет. Як у незалежній схемі, так і в СМС виконується одне хешування. Додаткові операції пов'язані переважно з конкатенацією службових полів, порівнянням Previous Hash та оновленням стану, порівняння наведено в табл. 2. Відносні додаткові ресурсні витрати для певного показника X визначаються як (5).

$$O_X = \frac{x_{CMC} - x_{ind}}{x_{ind}} \cdot 100\% \quad (5)$$

Експериментальне середовище складалося з трьох компонентів. Мікроконтролер STM32F407 використовувався як джерело телеметрії та формував повідомлення відповідно до запропонованої структури. ESP32-S3 виконував функцію комунікаційного шлюзу та передавав дані через Wi-Fi. Цифровий двійник реалізовано як програмний емулятор на персональному комп'ютері, на якому виконувались перевірка отриманих пакетів та підтримання криптографічного стану. Вбудоване програмне забезпечення реалізовано з використанням FreeRTOS. Окремі задачі забезпечували отримання сенсорних значень, формування телеметричного пакета, криптографічну обробку, передавання та синхронізацію.

Таблиця 2

Порівняння незалежного та каскадного хешування

Критерій	Незалежне хешування	Каскадне хешування
Обчислювальна складність	O(n)	O(n)
Вимоги до RAM	O(1)	O(1)
Вимоги до Flash	низькі	низькі
Хеш-операцій на пакет	1	1
Додаткові службові дані	відсутні	Previous Hash + службові поля
Модифікація	виявляється	виявляється
Вставлення	не контролюється	виявляється
Видалення	не контролюється	виявляється
Replay	обмежений контроль	виявляється
Перестановка	обмежений контроль	виявляється
Об'єкт перевірки	пакет	потік

Як полегшену хеш-функцію використано ASCON-Hash256, результатом якої є 256-бітне значення. Тому Previous Hash та Current Hash займають по 32 байти. Архітектуру експериментального середовища наведено на рис. 3.

Експеримент проводився для потоків із 10 000 послідовних телеметричних пакетів. Розглядалися пакети розміром 64, 128 та 256 байт, що дозволило оцінити метод для різного співвідношення прикладних і службових даних. У потік штучно вносилися порушення п'яти типів: модифікація пакета, вставлення, видалення, replay та перестановка. Для кількісного оцінювання ефективності використовувалися показники Detection Rate, Precision, Recall і F1-score. У відповідній серії експериментів близько 5% із 10 000 повідомлень навмисно піддавалися маніпуляціям. В кількісному експерименті з Detection

Rate вихідна стаття окремо наводить результати для modification, insertion, deletion і replay. Тому результати рис. 4 не слід штучно поширювати на перестановку пакетів, хоча цей сценарій передбачений загальною експериментальною постановкою.

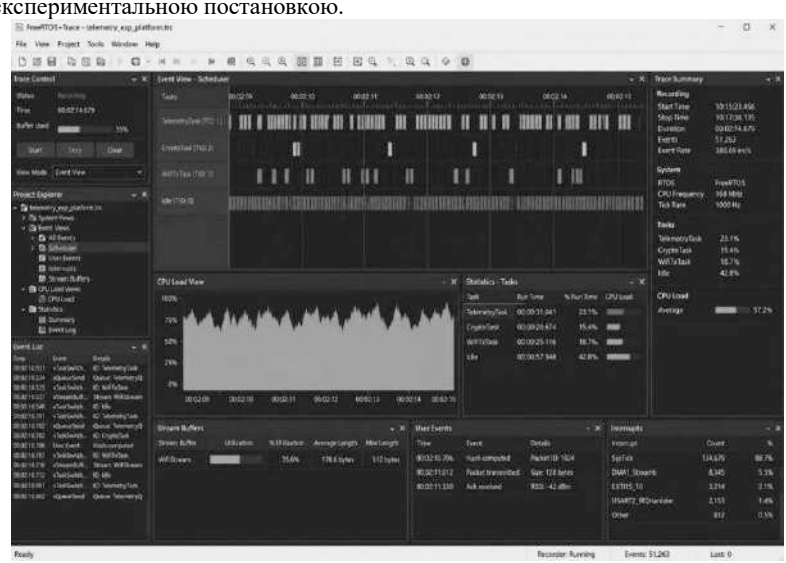


Рисунок 3. Експериментальна платформа передавання телеметрії та контролю її цілісності

5 Результати дослідження та аналіз стійкості методу

Результати ресурсного оцінювання наведено у табл. 3. Кожне значення отримано за однакових експериментальних умов для потоку з 10 000 повідомлень.

Таблиця 3

Порівняння ресурсних характеристик незалежного та каскадного хешування

Показник	Незалежне хешування	Запропонований метод	Зміна, %
Середній час обробки, мкс	142,8	151,6	+6,2
RAM, байт	416	448	+7,7
Flash, КБ	31,4	32,0	+1,9
Завантаження CPU, %	17,8	18,9	+6,2
Хеш-операцій на пакет	1	1	0
Обчислювальна складність	O(n)	O(n)	0

Середній час обробки одного повідомлення збільшився з 142,8 до 151,6 мкс, тобто на 6,2 %. При цьому кількість хеш-операцій залишилася незмінною. Отже, додаткові часові витрати зумовлені не повторним виконанням криптографічної функції, а підтриманням криптографічного стану та обробкою службових полів. Використання оперативної пам’яті збільшилося з 416 до 448

байт, тобто на 32 байти, або 7,7 %. Збільшення Flash-пам'яті становило 0,6 КБ, або 1,9 %. Завантаження процесора зросло з 17,8 до 18,9 %, що відповідає 6,2 %. Таким чином, найбільше відносне збільшення серед досліджуваних ресурсних показників спостерігалося для RAM, однак абсолютне збільшення становило лише 32 байти. Важливим результатом є збереження однакової асимптотичної складності та однакової кількості хеш-операцій. Це означає, що розширення області контролю від окремого пакета до послідовності не потребує пропорційного збільшення кількості криптографічних обчислень. Ефективність виявлення маніпуляцій із телеметрією наведено на рис. 4.

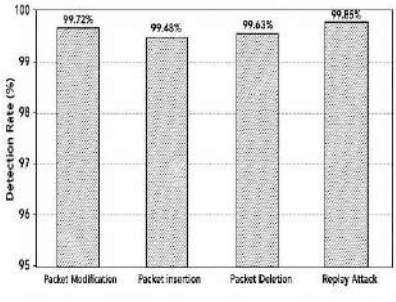


Рисунок 4. Рівень виявлення різних типів маніпуляцій із телеметричними повідомленнями

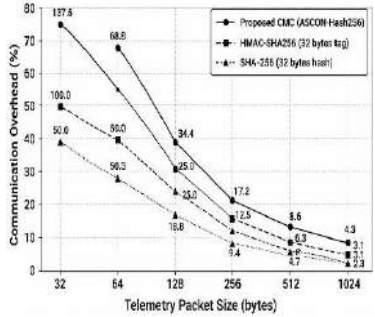


Рисунок 5. Значення Precision, Recall та F1-score для запропонованого методу контролю цілісності

Найбільш безпосередньо виявляється модифікація вмісту. Зміна D_i спричиняє зміну обчисленого H_i, тому отримане та очікуване контрольні значення перестають збігатися. При цьому наслідок не обмежується одним пакетом: непідтверджений стан не повинен використовуватися як основа для подальшого оновлення ланцюга. Вставка стороннього пакета змінює очікуваний перехід між двома сусідніми станами. Для легітимної послідовності криптографічна залежність має вигляд $H_{i-1} \rightarrow H_i \rightarrow H_{i+1}$. Вставка додаткового повідомлення порушує цей порядок, оскільки його Previous Hash або сформоване Current Hash не відповідають очікуваному стану приймача. При видаленні повідомлення наступний отриманий пакет містить Previous Hash вилученого елемента, тоді як приймач зберігає стан попереднього підтвердженого повідомлення. Отже, порушення виявляється ще до використання наступного пакета для актуалізації цифрового двійника.

Replay є складнішим випадком для незалежного хешування, оскільки повторно переданий пакет може залишатися криптографічно коректним. У CMC він перевіряється в контексті поточного стану. Previous Hash, Sequence Number та Timestamp старого повідомлення не відповідають поточній позиції телеметричного потоку. Аналогічний принцип застосовується до перестановки пакетів. Навіть якщо обидва повідомлення є легітимними, їх Previous Hash відповідають початковій, а не зміненій послідовності. Тому криптографічна зв'язаність дозволяє відрізняти правильний набір повідомлень від правильно

впорядкованого потоку. За результатами експериментів середні значення Precision, Recall та F1-score перевищили 99 %. Це підтверджує здатність механізму виявляти змодельовані маніпуляції за низького рівня хибних спрацьовувань.

Окрім обчислювальних витрат, СМС збільшує обсяг переданої інформації через включення службових полів. Цей показник особливо важливий для коротких телеметричних повідомлень. За результатами вихідного дослідження комунікаційний overhead зменшувався від 68,8 % для 64-байтових пакетів до 17,2 % для 256-байтових. Така залежність пояснюється фіксованим розміром основної частини службових даних. Зі збільшенням корисного навантаження їх частка у загальному розмірі повідомлення зменшується. Тому застосування повного формату СМС є вигіднішим з погляду відносного комунікаційного навантаження для більших телеметричних пакетів.

Для систем із дуже короткими повідомленнями цей показник необхідно враховувати окремо під час вибору формату передавання. Сукупний аналіз результатів демонструє, що основною перевагою запропонованого методу порівняно з незалежним хешуванням є не підвищення криптографічної стійкості самої хеш-функції, а розширення об'єкта контролю. Незалежне хешування відповідає на питання про незмінність конкретного інформаційного блока, тоді як СМС додатково перевіряє його належність до поточного стану телеметричного потоку.

При цьому метод має низку обмежень, які необхідно враховувати під час практичного застосування. По-перше, він потребує синхронізації криптографічного стану між сторонами. Часті природні втрати пакетів у нестабільному каналі можуть збільшувати кількість процедур ресинхронізації. По-друге, додаткові службові поля є суттєвими для малих пакетів. По-третє, запропонований механізм спрямований насамперед на цілісність і послідовність телеметрії та не замінює механізми конфіденційності або повноцінної автентифікації вузлів у системах, де такі властивості також є обов'язковими. Отримані експериментальні результати підтверджують придатність підходу до систем цифрових двійників, IIoT, Medical IoT, Smart Grid та edge-середовищ, для яких важливе поєднання контролю цілісності телеметрії з обмеженими ресурсами кінцевих пристроїв. Такі сфери застосування визначені й у вихідному дослідженні.

6 Висновки та перспективи подальших досліджень

У роботі запропоновано метод контролю цілісності потокових даних цифрових двійників на основі криптографічного зв'язування послідовних повідомлень. Необхідність його розроблення зумовлена тим, що традиційна незалежна перевірка телеметричних пакетів дозволяє встановити факт модифікації їхнього вмісту, але недостатньо враховує структурну цілісність потоку - порядок, повноту, часову актуальність та взаємозв'язок послідовних повідомлень.

Основою методу є механізм Cryptographic Message Chaining, відповідно до якого поточне хеш-значення формується на основі телеметричних даних, часової мітки, порядкового номера та хешу попереднього повідомлення. Це забезпечує одночасну залежність контрольного значення від вмісту поточного

пакета і попереднього криптографічного стану та дозволяє перейти від перевірки окремих пакетів до контролю криптографічно зв'язаної телеметричної послідовності. Запропонована конструкція не потребує зберігання повної історії повідомлень. Для формування та перевірки наступного стану достатньо останнього валідного хеш-значення, завдяки чому обсяг пам'яті криптографічного стану залишається сталим відносно довжини телеметричного потоку. Кількість хеш-операцій також не збільшується порівняно з незалежним хешуванням і становить одну операцію на пакет.

Експериментальну реалізацію виконано на основі STM32F407, ESP32-S3, FreeRTOS та ASCON-Hash256 для потоків із 10 000 повідомлень. Отримані результати показали збільшення середнього часу обробки пакета на 6,2 %, використання RAM – на 7,7 %, Flash-пам'яті – на 1,9 %, завантаження процесора – на 6,2 %. При цьому збережено лінійну обчислювальну складність та постійний обсяг пам'яті для підтримання стану.

Криптографічне зв'язування забезпечує виявлення не лише безпосередньої модифікації даних, але й порушень структури потоку, зокрема вставлення, видалення, повторного передавання та зміни порядку повідомлень. Значення Precision, Recall і F1-score у проведених експериментах перевищили 99 %. Водночас встановлено, що одним із компромісів є збільшення комунікаційних витрат, особливо для коротких телеметричних повідомлень: їх відносне значення зменшується від 68,8 % для пакетів розміром 64 байти до 17,2 % для 256 байт.

Таким чином, запропонований метод забезпечує компроміс між контролем структурної цілісності потокових даних і ресурсними витратами, що дозволяє використовувати його у вбудованих компонентах цифрових двійників. Подальший розвиток підходу доцільно спрямувати на адаптивне зменшення комунікаційних витрат для коротких пакетів, дослідження поведінки механізму в умовах нестабільних каналів із природними втратами повідомлень, апаратне прискорення криптографічних операцій, багатоканальну верифікацію телеметрії та дослідження можливості інтеграції з перспективними полегшеними криптографічними механізмами. У вихідній роботі серед подальших напрямів також визначено FPGA-реалізацію, постквантові полегшені хеш-алгоритми та багатоканальну перевірку телеметрії.

Література

[1] Qian, C., Liu, X., Ripley, C., Qian, M., Liang, F., & Yu, W. (2022). Digital twin—Cyber replica of physical things: Architecture, applications and future research directions. Future Internet, 14(2), 64. https://doi.org/10.3390/fi14020064

[2] Nadella, V. M. (2022). Digital Twins for Predictive Network Management and System Simulation. International Journal of AI, BigData, Computational and Management Studies, 3(3), 100–111. https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I3P112

[3] Kabir, M. R., Halder, D., & Ray, S. (2024). Digital twins for IoT-driven energy systems: A survey. IEEE Access, 12, 177123–177143. https://doi.org/10.1109/ACCESS.2024.3506660

[4] Faure, E., Rozlomii, I., & Naumenko, S. (2026). Hybrid digital twin-driven anomaly detection in IoT telemetry using LSTM autoencoder. Proceedings of the International

Workshop on Data Analytics (WDA'26), Kyiv, Ukraine, 76–89. https://doi.org/10.5281/zenodo.21155695

[5] Ali, W. A., Fanti, M. P., Roccotelli, M., & Ranieri, L. (2023). A review of digital twin technology for electric and autonomous vehicles. Applied Sciences, 13(10), 5871. https://doi.org/10.3390/app13105871

[6] Alsubaih, A. A. S., Sepehrnoori, K., Delshad, M., & Alsaedi, A. (2025). A comprehensive review of well integrity challenges and digital twin applications across conventional, unconventional, and storage wells. Energies, 18(17), 4757. https://doi.org/10.3390/en18174757

[7] Rozlomii, I., Yarmilko, A., & Naumenko, S. (2025). Innovative resource-saving security strategies for IoT devices. Journal of Edge Computing, 4(1), 35–56.

[8] Kose, K., Kose, N. A., & Liang, F. (2026). Securing unmanned devices in critical infrastructure: A survey of hardware, network, and swarm intelligence. Electronics, 15(6), 1204. https://doi.org/10.3390/electronics15061204

[9] Nouma, S. E., & Yavuz, A. A. (2024). Trustworthy and efficient digital twins in post-quantum era with hybrid hardware-assisted signatures. ACM Transactions on Multimedia Computing, Communications and Applications, 20(6), 1–30. https://doi.org/10.1145/363825

[10] Gautam, D., Thakur, G., Kumar, P., Das, A. K., & Park, Y. (2024). Blockchain assisted intra-twin and inter-twin authentication scheme for vehicular digital twin system. *IEEE Transactions on Intelligent Transportation Systems*, *25*(10), 15002–15015. https://doi.org/10.1109/TITS.2024.3394438

[11] Suleiman, R., Maradapu Vera Venkata Sai, A., Yu, W., & Wang, C. (2025). Blockchain for security in digital twins. *Future Internet*, *17*(9), 385. https://doi.org/10.3390/fi17090385

[12] Tang, Q., & Wu, B. (2024). A digital twin-driven multi-resource constrained location system for resource allocation. *The International Journal of Advanced Manufacturing Technology*, *130*(9), 4359–4385. https://doi.org/10.1007/s00170-023-12886-w

[13] Kamdjou, H. M., Baudry, D., Havard, V., & Ouchani, S. (2024). Resource-constrained extended reality operated with digital twin in industrial internet of things. *IEEE Open Journal of the Communications Society*, *5*, 928–950. https://doi.org/10.1109/OJCOMS.2024.3356508

[14] Khan, L. U., Han, Z., Saad, W., Hossain, E., Guizani, M., & Hong, C. S. (2022). Digital twin of wireless systems: Overview, taxonomy, challenges, and opportunities. *IEEE Communications Surveys & Tutorials*, *24*(4), 2230–2254. https://doi.org/10.1109/COMST.2022.3198273

[15] Yarmilko, A., Rozlomii, I., & Kosenyuk, H. (2021). Hash method for information stream's safety in dynamic cooperative production system. In *International Scientific-Practical Conference* (pp. 173–183). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-89902-8_14

[16] Wang, Q., Wu, W., Qian, L., Cai, Y., Qian, J., & Meng, L. (2023). Design and implementation of secure and reliable information interaction architecture for digital twins. *China Communications*, *20*(2), 79–93. https://doi.org/10.23919/JCC.2023.02.006

[17] Mitsenko, S., Naumenko, S., & Yarmilko, A. (2023). Information Protection and Recovery Hamming Codes Based'Hash Technique. In *Proceedings of the 11th International Conference "Information Control Systems & Technologies"*, Vol. 3513, 64–67. https://doi.org/10.5281/zenodo.21066947

[18] Ali, S., & Anwer, F. (2024). Secure IoT framework for authentication and confidentiality using hybrid cryptographic schemes. *International Journal of Information Technology*, *16*(4), 2053–2067. https://doi.org/10.1007/s41870-024-01753-w

[19] Mufidah, N. F., & Nuha, H. H. (2024). Performance and security analysis of lightweight hash functions in IoT. *Jurnal Informatika: Jurnal Pengembangan IT*, *9*(3), 264–270. https://doi.org/10.30591/jpit.v9i3.7633

[20] Țălu, M. (2025). Securing IoT ecosystems: Experimental evaluation of modern lightweight cryptographic algorithms and their performance. *Journal of Cybersecurity, 7*(1), 565. https://doi.org/10.32604/jcs.2025.073690

[21] Chowdhury, B., Jahankhani, H., & Subramaniam, S. (2023, October). Zero-trust blockchain-based digital twin 6G AI-native conceptual framework against cyber attacks for e-healthcare. In *International Conference on Global Security, Safety, and Sustainability* (pp. 453–479). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-82031-1_23

[22] Patil, D. A., & G, S. (2025). A comprehensive survey on securing the social internet of things: Protocols, threat mitigation, technological integrations, tools, and performance metrics. *Scientific Reports, 15*(1), 40190. https://doi.org/10.1038/s41598-025-23865-4

METHOD FOR INTEGRITY CONTROL OF DIGITAL TWIN DATA STREAMS BASED ON CRYPTOGRAPHIC CHAINING OF CONSECUTIVE MESSAGES

Ph.D., Rozlomii I.[1], Ph.D., Naumenko S.[2]

[1]Cherkasy State Technological University, Ukraine,

[2]Bohdan Khmelnytsky National University of Cherkasy, Ukraine

Abstract. *The widespread adoption of digital twin technologies in industrial, medical, energy, and other cyber-physical systems necessitates integrity control of continuous telemetry data streams generated by embedded devices and transmitted to update the digital representation of a physical object. Conventional independent hashing enables the detection of modifications to individual messages; however, it does not sufficiently account for the sequential nature of telemetry and has limited capabilities for detecting the insertion, deletion, replay, and reordering of valid packets. A method for integrity control of digital twin data streams based on cryptographic message chaining is proposed, in which the current hash value is generated using the payload, timestamp, sequence number, and cryptographic state of the preceding message. This transforms a set of independently verified packets into a cryptographically linked sequence and enables integrity control of both individual message contents and the structural consistency of the telemetry stream. The method does not require the complete message history to be stored, since only the latest valid hash value is required to generate the subsequent cryptographic state, thereby minimizing RAM usage regardless of the number of transmitted messages. The experimental implementation was performed using STM32F407, ESP32-S3, FreeRTOS, and ASCON-Hash256 for streams comprising 10,000 telemetry packets with sizes of 64, 128, and 256 bytes. Compared with independent hashing, the average packet processing time increased by 6.2%, RAM usage by 7.7%, Flash memory usage by 1.9%, and CPU utilization by 6.2%. Precision, Recall, and F1-score exceeded 99%. The obtained results confirm the applicability of cryptographic message chaining for integrity control of digital twin telemetry streams on resource-constrained embedded platforms.*

Keywords. *digital twin; data streams; telemetry; data integrity; lightweight cryptography; cascaded hashing; cryptographic message chaining; embedded systems; ASCON-Hash256*

Section 4 Modeling, software engineering, and applied ICT

UDK 519.642
DOI

A METHOD FOR VERIFYING THE ACCURACY OF COMPUTATIONAL IMPLEMENTATIONS FOR SOLVING DYNAMIC SYSTEM MODELING PROBLEMS

Dr.Sci., Polozhaenko S.[1][0000-0002-4082-8270], Dr.Sci., Fomin O.[2][0000-0002-8816-0652], Prokofieva L.[0000-0002-4045-2402], Ph.D., Prokofiev A.[0000-0002-4520-4248], Ph.D. Savieliev A.[0000-0002-6949-5959], Filin D.[0009-0000-6228-3657]

Odesa Polytechnic National University, Ukraine
EMAIL: [1]polozhaenko@op.edu.ua, [2]fomin@op.edu.ua

Abstract. *Modern control and simulation systems are critically dependent on computational resources that implement algorithms for real-time analysis of dynamic systems. This makes the development of lightweight and efficient algorithmic self-monitoring a pressing need. The goal of this work is to improve the quality and reliability of monitoring the computational process of numerically solving dynamic equations by applying auxiliary algorithmic procedures that run in parallel with the main algorithm but have lower computational complexity. Main objectives: to develop and justify criteria for detecting errors and failures in the operation of the main computational algorithm; to create a method for deciding whether to continue the computational process upon detection of discrepancies; to formulate and verify an interpolation method for real-time accuracy monitoring at the integration step. This work proposes a combined approach that includes a method with increasing computational accuracy: at each integration step, approximations of the state function are determined sequentially with an increasing order of accuracy for the local error. The use of previously computed derivatives at intermediate stages eliminates the need to recalculate computationally intensive right-hand sides of the system, thereby reducing the risk of failure. Accuracy is monitored indirectly by comparing the reference value with the result of an auxiliary formula. Results and practical significance: the interpolation method ensures higher accuracy of the reference.*

Ключові слова. *Dynamic systems, computational accuracy, numerical solutions, interpolation-based control methods, verification of mathematical models, fault detection, decision making.*

1 Introduction

A characteristic feature of modern control systems is the widespread use of various types of computing systems that implement modeling and control methods and algorithms. Therefore, the quality of operation of modeling and control systems is largely determined by the characteristics of the computing resources used. The problem of ensuring the quality of operation-in particular, of control systems with a computer in the control loop-is very complex from both a technical and a mathematical standpoint. In addressing this problem, practical experience has brought to the forefront a field of research focused on developing methods and tools that ensure the reliability of computational and information processing operations [1]. In real-world modeling or control systems, computational processes are inevitably accompanied by various types of disturbances and errors. For example, when performing numerical analysis of equations (or other mathematical relationships)

describing the dynamics (which constitute the state equations of a dynamic system) on a digital computer, errors in solving these equations (or other relationships) may, among other things, be caused by hardware malfunctions and failures. In this context, disturbances are defined [2] as distortions in the processed and control information caused by self-correcting root causes (incorrect operation of binary hardware elements, interference, power supply voltage fluctuations, etc.). Moreover, most disturbances are random in nature. Therefore, effective real-time monitoring is required to detect and eliminate errors before they propagate through the control loop, making responsiveness one of the key characteristics of error control systems.

2 Literature Review

An effective framework for describing dynamic processes in continuous systems when solving direct (modeling), reverse (control), and inverse (identification) problems are differential and integral equations [5]. This is due to the inherent nature of these types of mathematical expressions and the presence of an independent time parameter that characterizes the dynamic behavior of the systems under study. However, it should be noted that certain difficulties arise when solving differential and integral equations, which, in the course of modeling and controlling dynamic systems, are considered as mathematical models (MM) of these systems [6]. In particular, when solving differential equations, convergence problems may arise, and when solving integral equations, solutions may be ill-posed (for example, for Volterra and Fredholm equations of the first kind) [5]. One of the key indicators of the performance of computational tools used to solve differential and integral equations – for which there is currently no universal solution – is the assessment of the accuracy of solutions to modeling and control problems using the existing fleet of computers [7]. However, despite the widespread use of computing technology, the problem of assessing computational accuracy cannot be considered solved, and its relevance is growing due to the rapid development and proliferation of cybernetic tools for various purposes [8]. The severity of the problem lies in the complexity of analyzing computational errors, which leads to cumbersome analytical justifications and a large volume of computations required to obtain specific numerical data. Both general-purpose and specialized computing technology (CT) tools are widely used to solve many technical and research problems. A characteristic distinction between the latter and general-purpose CT tools is the intentionally narrow class of algorithms implemented, which is focused on solving a limited range of applied problems [9]. Naturally, this is expected to yield a number of specific advantages (compared to general-purpose CT tools), which typically include one or a group of factors such as increased speed, a non-analytical approach to problem-solving (for analog specialized CT tools), reduced size and weight, and lower cost, among others [10]. It should be noted that the issue of accuracy is relevant for both general-purpose and specialized CT tools, albeit in slightly different forms depending on the type of tool and its operating principle; for example, the nature of initial errors [11]. Thus, at present, when solving the vast majority of problems in the practice of modeling dynamic systems and synthesizing control for them, a contradiction is observed: while there is well-developed modeling and methodological support for MM of industrially important and environmentally significant dynamic systems [12], the issues of assessing the accuracy and reliability of solutions to the corresponding equations as

models of dynamic systems, as well as detecting failures (errors) in the computational process, have not been sufficiently developed [13].

The proposed method therefore differs from conventional sensitivity analysis and direct error estimation by introducing an intermediate layer of reference accuracy classes and correction coefficients. The objective is not to replace rigorous error bounds, but to use them to construct reusable accuracy classes that can support rapid assessment of new computational problems.

The main research gap addressed in this work is therefore the absence of a unified procedure that combines probabilistic error characterization, guaranteed bounds, reference-class construction, and computational ranking for the subsequent rapid assessment of dynamic-system model implementations.

3 Purpose and Objectives of the Study

The purpose of this work is to improve control over the computation process for any methods of numerical solution of dynamic equations by developing algorithmic control methods based on the application of a control algorithm that is executed during the numerical solution of the given (main) problem, but which is simpler than the main problem itself.

To achieve this purpose, the following tasks have been set:

– to propose criteria that allow one to conclude whether an error is present (or absent) in the main algorithm for the numerical implementation of the dynamic system's mathematical models, thereby enabling the detection of failures in the operation of the main computational algorithm;

– to develop a decision-making method that determines the presence or absence of a failure and makes a decision regarding the further course of the computational process for performing practical calculations when organizing the control of the computational process.

4 Development of a method for verifying the reliability of computational implementations of dynamic system models

4.1 Determining the possibilities for monitoring algorithms for the numerical solution of problems in the computational implementation of dynamic system models

Numerical methods for solving dynamic equations (or other mathematical relations that form the system of equations of dynamic systems) are a *step-by-step* procedure for obtaining the desired function. In this process, the computational process is naturally divided into time-invariant segments corresponding to the determination of the desired function at a specific integration step. Furthermore, the computational process is divided within each integration step into time-invariant segments that correspond to the determination of the values of the right-hand side of the system of equations being solved (using the example of a dynamic system modeled as a differential equation)

$$Y = f(Y,U,t), Y(t_0) = Y_0 \quad (1)$$

where $Y = (y_1, y_2, ..., y_n)^T$ is the vector of state variables; $U = (u_1, u_2, ..., u_n)^T$ is the vector of control signals; $f = (f_1, f_2, ..., f_n)^T$ is the vector-function; t is the independent time parameter.

Let us consider the capabilities of the numerical solution procedures (1) regarding the organization of control (self-control) of computational processes. To organize control (self-control), reference values are required against which the calculation results are compared. Verified results from previous calculations or results obtained with a low probability of failure can be used as reference values.

For any methods of numerically solving dynamics equations of the form (1), failure control can be organized by comparing the results obtained at the current and subsequent integration steps, respectively. The presence or absence of failures is determined by checking the condition

$$\xi = \rho\left(y_i, y_{i+1}\right) \in D \tag{2}$$

where ξ is a measure of the proximity of the values y_i and y_{i+1}; D is the domain of valid values for this measure.

To control errors caused by divergences and failures, methods for controlling the systematic error of the numerical solution at the integration stage or specific features of the design of computational algorithms can be used.

In the prediction and correction methods [13–16], based on the difference $\xi = |y_f - y_c|$ between *the* predicted y_f and the corrected y_c values of the function of interest, conclusions can be drawn regarding the presence of a malfunction in the equipment. However, the existing correlation between the values y_f and y_c undermines the reliability of the control.

Let us illustrate this using the example of the improved Euler–Cauchy method [17, 18]. Suppose the prediction is performed according to the formula:

$$y_{i+1} = y_i + hf_i, \tag{3}$$

where h is the integration step; $f_i = f(Y, U, t_i)$, and the correction is performed according to the expression

$$y_{i+1} = y_i + \frac{h}{2}\left(f_i + \tilde{f}_{i+1}\right) \tag{4}$$

where $\tilde{f}_{i+1} = f\left(\tilde{\mathbf{Y}}, \mathbf{U}, t_{i+1}\right)$.

As can be seen from (3) and (4), the function $f\left(\tilde{\mathbf{Y}}, \mathbf{U}, t_{i+1}\right)$ is computed twice per integration step at the points t_i and t_{i+1}. Since this process typically accounts for the bulk of the computational work, let us assume that a failure occurred at the moment of calculating $f\left(\tilde{\mathbf{Y}}, \mathbf{U}, t_{i+1}\right)$ and the value of the function f_i was obtained with an error *of* Δf_i. Then the value of the function that can be obtained according to formula (3) will be

$$\tilde{y}_{i+1} = y_i + h\left(f_i + \Delta f_i\right) = y_i + h\, f_i + h\Delta f_i \tag{5}$$

Here, $\Delta y_{i+1} = h\Delta f_i$ is the error in the forecast value. Let's calculate the value of the function y_{i+1} according to formula (4)

$$y_{i+1} = y_i + \frac{h}{2}\left[\left(f_i + \Delta f_i\right) + f_i + \frac{\partial f_i}{\partial y} h_i\left(f_i + \Delta f_i\right) + \frac{\partial f_i}{\partial t} h\right] \tag{6}$$

The difference between the predicted (5) and corrected (6) values will be equal to

$$\xi = |\tilde{y}_{i+1} - y_{i+1}| = \frac{h}{2}\left|\Delta f_i\left(1 - \frac{\partial f_i}{\partial y}h\right) - h\left(\frac{\partial f_i}{\partial y}f_i + \frac{\partial f_i}{\partial t}\right)\right| \quad (7)$$

from which it follows that the value ξ depends on the values of the derivatives $\partial f_i/\partial y$ and $\partial f_i/\partial t$.

In contrast to modified prediction and correction methods, we propose a method *with increasing computational accuracy*, the essence of which lies in sequentially obtaining the value of the function at the integration step with an increasing order of accuracy of the local error (the essence being the error at the integration step). It is clear that for an arbitrary order of accuracy, *r*, we can write:

$$y_{i+1}^{(r)} = y_i^{(r)} + \frac{h}{2}\left[f\left(y_i^{(r)}, u_i, t_i\right) + f\left(y_{i+1}, u_{i+1}, t_{i+1}\right)\right] \quad , \quad (8)$$

$$y_{i+1}^{(r-1)} = y_i^{(r)} + h\, f\left(y_i^{(r)}, u_i, t_i\right), \quad (9)$$

where the superscript indicates the order of the local error of the approximate value.

By comparing the values of $y_{i+1}^{(r-1)}$ and $y_{i+1}^{(r)}$, one can draw conclusions about the local error in the solution. This same technique can also be used to detect errors caused by failures. Thus, if there was no failure in the previous step, an error in determining $y_{i+1}^{(r-1)}$ can occur only if expression (9) holds.

Given the computational complexity—and, consequently, the probability of failure—for procedures (8) and (9), this probability is lower than for other *single-step* methods of the same order of accuracy with respect to the step size *h*. Additionally, since the probability of failure when computing $y_{i+1}^{(r-1)}$ is significantly lower than the probability of failure when computing the function *f*(*y*,*u*,*t*), when the latter has a complex form, it is advisable (from the perspective of error control) to organize the control process using a method *with increasing* second-order *computational accuracy*, i.e., (r-1)=2.

The described process can be easily implemented, for example, in the second-order accuracy method (r-1)=2 using expressions (8) and (9). In this case, when calculating $y_{i+1}^{(2)}$, the function *f*(*y*,*u*,*t*) is not computed; instead, the value $f\left(y_{i+1}^{(2)}, u_{i+1}, t_{i+1}\right)$ obtained in the previous integration step is used, which significantly reduces the probability of an error occurring when calculating the value $y_{i+1}^{(2)}$. An algorithm that implements the method *with increasing computational accuracy* must meet the following requirements:

1. The calculation process at each integration step must begin with determining the function f at the point t_{i+1} . In this case, the function $f(y,u,t_{i+1})$ is not computed; instead, the value of the function *f* obtained and verified during the calculation of the most accurate solution to system (1) at the previous integration step is used. The calculation formula for obtaining the first approximate value $y(t_i + h)$ with a local error *of* $O(h^2)$ is given by

$$y_{i+1}^{(2)} = y_i^{(r)} + h\, f\left(y_i^{(r-1)}, u_i, t_i\right), \quad (10)$$

where r is the order of the local error of the approximate solution; $f\left(y_i^{(r-1)}, u_i, t_i\right)$ is the estimate of the derivative used in determining $y_i^{(r)}$.

If we disregard the single-step condition and incorporate information about the problem being solved over an interval longer than the integration step h, we can increase the order of accuracy of the first approximate value of the function $y(t_i + h)$. When constructing a *multi-step* procedure to obtain the first approximation of the function at the point t_{i+1},one can use estimates of the derivative of the function $\frac{\partial f(y+\Delta y, u, t_{i+1})}{\partial y}$ obtained within the step $[t_{i-1}, t_i]$. The correctness of the calculations according to (8) is verified by checking the condition

$$\xi \in D, \tag{11}$$

where $\xi = \xi\left(y_{i+1}^{(2)}, y_{i+1}^{(3)}\right)$ – the measure of computational accuracy; D – the permissible range of values for this measure.

If condition (10) is not satisfied, the incorrect solution is corrected by recalculating the values of $y_{i+1}^{(3)}$, or by replacing $y_{i+1}^{(3)}$ with $y_{i+1}^{(2)}$. In the latter case, an error will be introduced, which is determined by the difference between the residual terms in the corresponding formulas and is a small quantity of the order of $O(h^2)$. In this case, the correction time will be a random variable with a mathematical expectation of

$$M\left[T_{\text{кор}}\right] = \left(t_{\text{наб}} + t_{\text{оп.к}}\right)\sum_{m=0}^{H} C_H^m p^m q^{H-m} \tag{12}$$

where t_{comp} – the time required to compute the next approximation of the function $y(t)$ at point t_{i+1} ; t_{check} – the time required for the check operation; $H = kN$ (k is the number of divisions required to obtain a solution with increasing accuracy, N is the number of integration steps); p is the probability of failure when computing the next approximation; $q = 1 - p$.

The expected value of the total solution time for N calculation steps is

$$M[T] = H\left(t_{\text{наб}} + t_{\text{оп.к}}\right) + M\left[T_{\text{кор}}\right] \tag{13}$$

If the correction is performed by replacing the incorrect value of $y_{i+1}^{(r)}$ with the value of this function at the point t_i+1 that is closest in accuracy, then an error will be introduced into the solution

$$\xi = y_{i+1}^{(l+1)} - y_{i+1}^{(l)} = \eta_{i+1}^{(l+1)} - \eta_{i+1}^{(l)} \tag{14}$$

where $y_{i+1}^{(l)}$ and $y_{i+1}^{(l+1)}$ are successive approximations of the function $y(t)$ with local error orders l and (l+1), respectively; $\eta_{i+1}^{(l)}$ and $\eta_{i+1}^{(l+1)}$ are small quantities with smallness orders h^l and h^{l+1} respectively.

2. The number of partitions k (i.e., the number of values $y_{i+1}^{(r)}$ obtained with increasing accuracy on the interval $[t_i, t_{i+1}]$) can be chosen by minimizing (11) subject to the constraint on the value of $\xi = \left(y_{i+1}^{(l+1)} - y_{i+1}^{(l)}\right)$, or conversely, by minimizing ξ

subject to the constraint on $M[T]$. However, in practice, $t_{\text{наб}} >> t_{\text{оп.к}}$, and therefore, when designing an algorithm for the method with increasing accuracy, it is advisable to choose the maximum number of partitions k that is possible for the method of the selected accuracy order r. Let us estimate the leading term of the error using Runge's rule [18, 19]. In this case, the application of this rule boils down to the following. For a given point t on the interval $[t_0, t_N]$, using the kth-order accuracy method, we can sequentially obtain the approximate values of the function y_{h_1} and y_{h_2} at steps $h_1 \neq h_2$, respectively. Let us define the quantity:

$$\xi(t) = \frac{y_{h_1} - y_{h_2}}{h_2^k - h_1^k} \tag{15}$$

Then, taking into account the magnitude of the leading term of the error for each of the values $h=h_1$ and $h=h_2$

$$\xi_1 = h_1^k \frac{y_{h_1} - y_{h_2}}{h_2^k - h_1^k} \text{ and } \xi_2 = h_2^k \frac{y_{h_1} - y_{h_2}}{h_2^k - h_1^k}, \tag{16}$$

we can draw conclusions regarding the accuracy of the calculations.
With a uniform step size for the interval $[t_0, t_N]$, that is, if $h_1 = h$ and $h_2 = 2h$, the expression for the leading term of the error takes the following form:

$$\xi = y - y_h \approx \frac{y_h - y_{2h}}{2^k - 1} \tag{17}$$

Depending on the calculated value of ξ, to achieve the specified accuracy, the step size h must either be decreased or increased (although in the latter case, the calculated accuracy will exceed the specified accuracy, the computation time may increase significantly, and the convergence of the solution may deteriorate).

An error caused by a failure and exceeding the permissible value of the leading term of the error estimate ξ_{perm} will be detected and eliminated by recalculating with a reduced step size h. The Runge rule [15] requires additional computations, which significantly increases the time required and the probability *of first-kind* errors (also known as α-errors, i.e., a false-rejection conclusion is drawn, leading to the rejection of a true hypothesis), and therefore the application of this rule in control systems is problematic (or even unacceptable). It should also be noted that the use of variable step size in calculations – that is, $h \neq \text{const}$ — in control systems is further complicated by the presence of control signals, which must be either pre-stored or calculated using interpolation formulas when the step size h changes, introducing an additional error into the solution. Therefore, when evaluating computational errors for control systems, we will demonstrate the possibility of applying *quadrature formulas*. We will use the values y_i and $i = \overline{1, N}$ obtained using the main algorithm, applying the following quadrature formula

$$y(t_i) = y_0^* + \int_{t_0}^{t_N} f(y^*, u, t)dt \tag{18}$$

where y* is the exact value of the function, and then we can obtain

$$\bar{y}_N = y_0^* + \sum_{i=0}^{N} A_i f(y_i, u_i, t_i), \quad (19)$$

where A_i are constant coefficients.

The conclusion regarding the presence of an error is made by checking the condition:

$$\xi = |y_N - \bar{y}_N| \le \xi_{\text{доп}} \quad (20)$$

where ξ_{tol} is the permissible value of the error ξ.

Below, we propose algorithmic control methods [17] that can be applied to control the computation process for any method of numerical solution of dynamic equations. In addition, we will consider control based on the application of an additional (verification) algorithm at each step of the numerical solution of the dynamic equation.

4.2 Interpolation-Based Control Method

When using the extrapolation control method, it is possible to correct the solution not by repeating the calculations, but by replacing y_{i+1} with $\bar{y}_{i+1}$, which is essential for modeling and control on a real-time (or accelerated) time scale. However, the accuracy of the control in this case depends on the accuracy of the solution extrapolation using Equation (22) and may prove unsatisfactory.

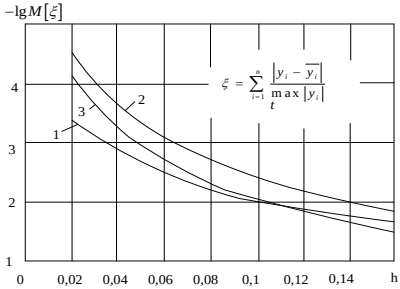


Figure 1. Dependence of the mathematical expectation $M[\xi]$ of the variable ξ on the step size h

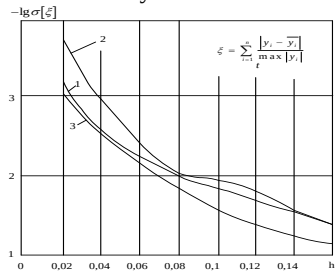


Figure 2. Dependence of the mean square error $\sigma[\xi]$ of the variable ξ on the step size h

For this reason, from the perspective of improving control accuracy, the method based on the concept *of interpolation* should be considered superior to the extrapolation method [17]. Note that, unlike extrapolation formulas, interpolation control formulas account for *the change in the solution at the controlled calculation step*, which leads to *a reduction in the difference* between the values y and $\bar{y}$, which result from the application of algorithms $\boldsymbol{A}_0$ and $\boldsymbol{A}_k$, respectively. The accuracy of the interpolation can be improved by incorporating the results of calculations using the main algorithm $\boldsymbol{A}_b$ up to the calculation step being controlled. To increase *the sensitivity* of error *control* caused by disruptions, one should use a control interpolation formula to determine the function value obtained at the calculation step closest to the controlled calculation step.

In light of the above, we propose a control-based multi-step interpolation formula that can be used to monitor the computation process at the (i+1)-th step:

$$\bar{y}_i = \sum_{p=-1}^{p_1} a_p y_{i-p} + h \sum_{s=-1}^{s_1} b_s f(\mathbf{Y}, \mathbf{U}, t_{i-s}), \quad (21)$$

where a_p and b_s are real coefficients; $p \neq 0$ (this is a degenerate case in which a_0=1 and all other coefficients are zero, and the identity $\bar{y}_i \equiv y_i$ holds).

As in the case of the extrapolation formula (22) in (29), the upper limits of summation must be chosen depending on the required order of control accuracy, and the coefficients a_p and b_s must be chosen based on the accuracy of the representation of polynomials of the corresponding degree.

Thus, expression (21) defines the procedure for *the interpolation method of* calculation control [12]. The fundamental difference between the interpolation expression (21) and the extrapolation expression (22) as control algorithms lies in the following. In the case of extrapolation formulas, the directly controlled quantity is the function value obtained using the main algorithm $\boldsymbol{A}_b$ at the controlled calculation step, and the control value is the result of applying expression (22). In the case of interpolation control formulas, the value $\bar{y}_i$ is calculated using expression (21), and the reference value is the function value obtained using the main algorithm $\boldsymbol{A}_b$ at the previous (*i-p*)-th calculation step; that is, *indirect* control is essentially performed. The error in calculating the value $\bar{y}_{i+1}$ using the main algorithm $\boldsymbol{A}_b$ is transformed into the error $\Delta\bar{y}_i$ in determining $\bar{y}_i$ according to formula (21). The deviation in $\Delta\bar{y}_i$ in this case, within the framework of linear accuracy theory, will be defined as

$$\Delta\bar{y}_i = L\eta, \quad (22)$$

where $L = \partial\bar{y}_i / \partial y_{i+1}$.

When applied to expression (21), L is determined by the formula

$$L = a_* - b_* h \frac{\partial f(\mathbf{Y}, \mathbf{U}, t_{i+1})}{\partial y_{i+1}}, \quad (23)$$

where a_* and b_* are coefficients, with y_{i+1} in (21).

$$\xi_i = \left\{ \sum_{j=1}^{p} \left[\left(y_{i,j} - \bar{y}_{i,j} \right) \Big/ \left(\max_i |y_j| \right) \right]^2 \right\}^{1/2}, \quad (24)$$

on the discretization step *size h* in Equation (1), which describes the flight dynamics of an aircraft. Curves 1 and 2 were obtained using first- and second-order interpolation formulas, respectively, at the (i+1)-th calculation step according to the basic algorithm $\boldsymbol{A}_b$:

$$y_i = y_{i+1} - h\dot{y}_{i+1} \quad (25)$$

$$\bar{y}_i = y_{i+1} - 0.5h(y_{i+1} + y_i), \quad (26)$$

For comparison, curve 3 is shown, corresponding to the use of the extrapolation formula

$$\bar{y}_{i+1} = y_i + h(2.25y_{i-1} - 1.25y_{i-2}) \quad (27)$$

It can be seen that as the discretization step size h increases, the accuracy of the interpolation control method increases compared to the extrapolation method.

The interpolation control method allows for increased accuracy in obtaining reference values. However, when organizing the control of a computational process, it should be borne in mind that when using the interpolation control method, it is not possible to replace an erroneous value obtained using the main algorithm $\boldsymbol{A}_b$ with a value obtained using the control algorithm $\boldsymbol{A}_k$ (which is possible with the extrapolation method).

4.3 Constructing "lower" estimates of the distribution laws of the non-removable error based on the use of guaranteed estimates

Hereinafter, we will assume that the excitation elements ΔA and Δb are random variables with known probability characteristics. The lower-bound distribution law for the quantities $\| \Delta x \|$ and $\| \Delta x \| / \| x \|$ (i.e., those that determine the accuracy of the solution to equation (8)) can be obtained by determining the distribution law of the right-hand side of the corresponding guaranteed error. Without loss of generality, we will consider the following estimates:

– for absolute errors

$$\| \Delta x \| \leq \frac{\| A^{-1} \| (\| \Delta A \| \cdot \| x \| + \| \Delta b \|)}{1 - \| A^{-1} \| \cdot \| \Delta A \|}, \tag{28}$$

– for relative errors

$$\frac{\| \Delta x \|}{\| x \|} \leq \frac{\| A^{-1} \| \cdot \| A \| (\frac{\| \Delta A \|}{\| A \|} + \frac{\| \Delta b \|}{\| b \|})}{1 - \| A^{-1} \| \cdot \| \Delta A \|} \tag{29}$$

In the first case, the random variable of interest is a function of two random variables $\| \Delta A \| \cdot \| \Delta b \|$ and non-random parameters $A^{-1} \cdot \| x \|$. In the second case, it is a function of the same random variables and non-random parameters $\| A^{-1} \|, \| A \| \cdot \| b \|$. It should be noted that the values $A^{-1} \cdot \| x \|$ are, as a rule, unknown.

To solve the given problem, it is necessary to know the distribution functions of the random variables $\| \Delta A \| \cdot \| \Delta b \|$. To find them, we propose the following procedures.

1. Let there be an n-dimensional vector Δb, whose components Δb_i and $i = \overline{1, n}$ are random variables with distribution functions $F_i(\tau)$. We need to:

– Find $F_{\| \Delta b \|_2}(\tau)$

$$F_{\| \Delta b \|_2}(\tau) = \begin{cases} \prod_{i=1}^{n} F_i(\tau) - F_i(-\tau)], \tau > 0; \\ 0, \tau \leq 0. \end{cases} \tag{30}$$

– Determine $F_{\| \Delta b \|_2}(\tau)$:

$$F_{\| \Delta b \|_2}(\tau) = P\{\sum_{i=1}^{n} \Delta b_i \mid \leq \tau\} \tag{31}$$

2. Let there be an ($n \times n$) matrix ΔA, whose components Δa_{ij} and $i, j = \overline{1,n}$ are independent continuous random variables with distribution functions $F_{ij}(\tau)$. We need to:

– determine $F_{\|\Delta b\|_2}(\tau)$:

$$F_{\|\Delta b\|_2}(\tau) = \begin{cases} \prod_{i=1}^{n} F_i^*(\tau), \tau > 0; \\ 0, \tau \le 0. \end{cases} \quad (32)$$

where $F_i^*(\tau)$ is the distribution function of the random variables ξ_i.

– Determine $F_{\|\Delta b\|_2}(\tau)$:

$$F_{\|\Delta b\|_2}(\tau) = \begin{cases} \prod_{j=1}^{n} F_i^{**}(\tau), \tau > 0; \\ 0, \tau \le 0. \end{cases} \quad (33)$$

where $F_i^{**}(\tau)$, $j = \overline{1,n}$ is the probability mass function of the random variables.

A coarser but easily computable lower bound can be constructed by determining the probability of landing within a rectangle with sides parallel to the coordinate axes and vertices at the points $(\tau_{1\min}, \tau_{2\min}), (c, \tau_{2\min}), (\tau_{1\min}, \alpha), (c, \alpha)$. It is advisable to take the point of intersection of the lines $\frac{\tau_1 + \tau_2}{\mu - \tau_1} = const$ and $\tau_1 = \gamma\tau_2$ as the point c, α, where $\gamma = \tau_{1\min}$ (Fig. 3, a, b).

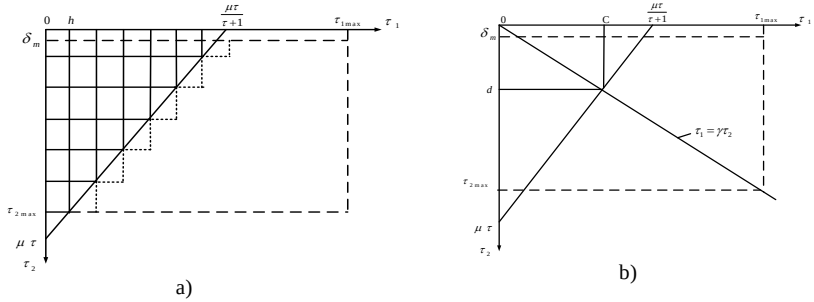


Figure 3. Construction of the lower bound of the estimate of the non-removable error, a – graphical determination of the distribution $F_{\|\cdot\|}(\tau)$; b – determination of a "rough" estimate of the lower bound

.

In this case,

$$\mu = \frac{1}{\| A^{-1} \|_1 \cdot \| A \|_1}; c = \frac{\tau\gamma\mu}{1 + \gamma(1+\tau)}; \alpha = \frac{\tau\mu}{1 + \gamma(1+\tau)} \quad (34)$$

When solving a system of linear algebraic equations, the matrix ΔA and the vector Δb depend on the method of inputting the input data. However, in any case,

it can be assumed that the matrix ΔA and the vector Δb coincide with the error matrix and error vector for the coefficients of the corresponding elements of matrix A and vector b.

5 Conclusion

The possibilities for verifying the accuracy of the computational implementation of dynamic systems' mathematical models during their modeling and control processes have been identified.

A method with increasing computational accuracy is proposed, which, unlike the basic and modified methods of prediction and correction, allows for the sequential (in particular, at individual integration steps) determination of the values of the sought state function of dynamic systems with an increasing order of accuracy of the local error.

Moreover, the order of accuracy can be specified in advance, prior to the execution of the main stages of the numerical implementation of the mathematical models for a dynamic system.

Algorithmic control methods are proposed that can be applied to control the computation process for any method of numerically solving equations of dynamics, namely: extrapolation and interpolation control methods. These methods are based on the use of a control algorithm that is executed during the numerical solution of the given (main) problem, but which is simpler than the main problem itself. The difference between these methods lies in the fact that the extrapolation method allows for an increase in the accuracy of the calculations by using, within the control algorithm, information that has already been verified in previous steps of the main algorithm, while the interpolation method enables the implementation of implicit control, which reduces the range of deviation of the controlled variable from the reference value-that is, it reduces the noise level.

Criteria are proposed that allow one to conclude whether an error is present (or absent) in the main algorithm of the numerical implementation of a dynamic system's mathematical models, thereby enabling the detection of malfunctions in the main computational algorithm.

This has made it possible to develop adaptive methods for verifying the accuracy of the numerical implementation of dynamic systems mathematical models; these methods ensure the determination of the control algorithm's parameters based on the condition of minimizing a selected measure of proximity between the results obtained using the control algorithm and the main algorithm for the numerical implementation of dynamic systems mathematical models.

To perform practical calculations when organizing the control of the computation process, a decision-making method is proposed whereby the presence or absence of a failure is determined and a decision is made regarding the further course of the computational process.

The method is based on taking into account the degree of divergence (or discrepancy) between the values obtained using the main and control algorithms, as well as setting a tolerance for this degree of divergence and subsequently selecting a strategy for continuing the computational process.

References

1. Castro R., Bergonzi M., Pecker Marcosig E., Fernández J., Kofman E. Discrete-event simulation of continuous-time systems: Evolution and state of the art of quantized state system methods. Simulation. 2024. Vol. 100, No. 6. P. 613–638. DOI: https://doi.org/10.1177/00375497241230985.

2. Nouaime N., Després B., Puscas M. A., Fiorini C. Stability of a continuous/discrete sensitivity model for the Navier–Stokes equations. International Journal for Numerical Methods in Fluids. 2024. Vol. 96, No. 12. pp. 1883–1909. DOI: https://doi.org/10.1002/fld.5324.

3. Gani R., Eden M. R., Perkins J. D., et al. Models, modeling, and model-based systems in the era of computers, machine learning, and AI. Computers & Chemical Engineering. 2025. Vol. 194. Art. 108957. DOI: https://doi.org/10.1016/j.compchemeng.2024.108957.

4. Yavuz M., Dassios I. Significance of Mathematical Modeling and Control in Real-World Problems: New Developments and Applications. Mathematical and Computational Applications. 2024. Vol. 29, No. 5. Art. 82. DOI: https://doi.org/10.3390/mca29050082.

5. Wu Q., Sun M. An Efficient Nyström-Type Method for Solving Highly Oscillatory Volterra Integral Equations of the Second Kind. PLOS ONE. 2023. Vol. 18, No. 12. Article e0295584. DOI: https://doi.org/10.1371/journal.pone.0295584.

6. Dai X., Niu J., Xu Y. An efficient numerical algorithm for solving nonlinear Volterra integral equations in the reproducing kernel space. Journal of Applied Mathematics and Computing. 2023. Vol. 69. pp. 3131–3149. DOI: https://doi.org/10.1007/s12190-023-01874-8.

7. Lu Y., Liu J.-B., et al. Approximate solutions to several classes of Volterra and Fredholm integral equations using a neural network algorithm based on sine-cosine basis functions and an extreme learning machine. Frontiers in Computational Neuroscience. 2023. Vol. 17. Article 1120516. DOI: https://doi.org/10.3389/fncom.2023.1120516.

8. Sivalingam, S. M., Kumar, P., Govindaraj, V. A neural networks-based numerical method for generalized Caputo-type fractional differential equations. Mathematics and Computers in Simulation, 2023, Vol. 213, pp. 302–323. DOI: https://doi.org/10.1016/j.matcom.2023.06.012.

9. Saleh, M., Kovács, E., Nagy, Á. New stable, explicit, second-order hopscotch methods for diffusion-type problems. Mathematics and Computers in Simulation, 2023, Vol. 208, pp. 301–325. DOI: https://doi.org/10.1016/j.matcom.2023.01.029.

10. Taneja, K., Deswal, K., Kumar, D. A robust higher-order numerical technique with graded and harmonic meshes for the time-fractional diffusion–advection–reaction equation. Mathematics and Computers in Simulation, 2023, Vol. 213, pp. 348–373. DOI: https://doi.org/10.1016/j.matcom.2023.06.010.

11. Yang, X., Yang, Z., Zhang, C. Numerical analysis of the linearly implicit Euler method with a truncated Wiener process for the stochastic SIR model. Mathematics and Computers in Simulation, 2023, Vol. 208, pp. 1–14. DOI: 10.1016/j.matcom.2023.01.010.

12. Kumar, V., Pham, H. (Eds.) Predictive Analytics in System Reliability. Springer Series in Reliability Engineering, Springer, 2022. DOI: https://doi.org/10.1007/978-3-031-05347-4.

13. Wang, J., Zhang, C. “Reliability model of open source software considering fault introduction with generalized inflection S-shaped distribution.” *SN Applied Sciences*, 2022, Vol. 4, Article 244. DOI: https://doi.org/10.1007/s42452-022-05125-6.

14. Bernardi, S., Gómez, A., Merseguer, J., Perez-Palacin, D., Requeno, J. I. DICE simulation: a tool for software performance assessment at the design stage. Automated Software Engineering, 2022, Vol. 29, Article 36. DOI: https://doi.org/10.1007/s10515-022-00335-z.

15. Cabot, J., Vallecillo, A. Modeling should be an independent scientific discipline. Software and Systems Modeling, 2022, Vol. 21, pp. 2101–2107. DOI: https://doi.org/10.1007/s10270-022-01035-8.

16. Lu, J., Yang, Z., Zheng, X., Wang, J., Kiritsis, D. Exploring the concept of the Cognitive Digital Twin from a model-based systems engineering perspective. The International

Journal of Advanced Manufacturing Technology. 2022. Vol. 121. pp. 5835–5854. DOI: https://doi.org/10.1007/s00170-022-09610-5.

17. Giannetti, C., Essien, A. "Toward Scalable and Reusable Predictive Models for Cyber Twins in Manufacturing Systems." Journal of Intelligent Manufacturing. 2022. Vol. 33. pp. 441–455. DOI: https://doi.org/10.1007/s10845-021-01804-0.

18. Fomin O. O., Speranskyy V. O., Verlan A. A., Tataryn O. V., Chmelevskyi A. M. "Long Short-Term Memory-based reference model method for nonlinear dynamic system identification." Herald of Advanced Information Technology. 2026; Vol. 9, No. 3: 307–320. DOI: https://doi.org/10.15276/hait.09.2026.20.

19. Guo, J., Lv, Z. "Application of Digital Twins in Multiple Fields." Multimedia Tools and Applications. 2022. Vol. 81. pp. 26941–26967. DOI: https://doi.org/10.1007/s11042-022-12536-5.

20. Tao, F., Xiao, B., Qi, Q., Cheng, J., & Ji, P. (2022). Digital twin modeling. Journal of Manufacturing Systems, 64, 372–389. DOI: https://doi.org/10.1016/j.jmsy.2022.06.015.

21. Onaji, I., Tiwari, D., Soulatiantork, P., Song, B., & Tiwari, A. (2022). Digital twin in manufacturing: conceptual framework and case studies. International Journal of Computer Integrated Manufacturing, 35(8), 831–858. DOI: https://doi.org/10.1080/0951192X.2022.2027014.

22. Cabot, J., Vallecillo, A. Modeling should be an independent scientific discipline. Software and Systems Modeling, 2022, Vol. 21, pp. 2101–2107. DOI: https://doi.org/10.1007/s10270-022-01035-8.

23. Yavuz M., Dassios I. Significance of Mathematical Modeling and Control in Real-World Problems: New Developments and Applications. Mathematical and Computational Applications. 2024. Vol. 29, No. 5. Art. 82. DOI: https://doi.org/10.3390/mca29050082.

24. Prokofiev A. Yu. Precision calibration method in the implementation of mathematical models of dynamic systems in modelling and control problems. Mathematical and computer modelling. Series: Technical sciences: collection of scientific works, 2022. Issue 23. P 116-129. DOI https://doi.org/10.326226/2308-5916.2022-23.116-129.

25. Polozhaenko S. A., Prokofiev A. Yu. Parameters of the Runge-Kutta method with different orders of accuracy when integrating dynamics equations in modeling problems of non-stationary systems. Computer science and mathematical methods in modelling, 2024 Vol. 14, No. 1–2. P. 85–96. DOI https://doi.org/10.15276/imms.v14.no1-2.85.

26. Gani R., Eden M. R., Perkins J. D., et al. Models, modeling, and model-based systems in the era of computers, machine learning, and AI. Computers & Chemical Engineering. 2025. Vol. 194. Art. 108957. DOI: https://doi.org/10.1016/j.compchemeng.2024.108957.

27. Castro R., Bergonzi M., Pecker Marcosig E., Fernández J., Kofman E. Discrete-event simulation of continuous-time systems: Evolution and state of the art of quantized state system methods. Simulation. 2024. Vol. 100, No. 6. P. 613–638. DOI: https://doi.org/10.1177/00375497241230985.

28. Segovia, M.; Garcia-Alfaro, J. Design, Modeling, and Implementation of Digital Twins. Sensors 2022, 22, 5396. DOI: https://doi.org/10.3390/s22145396.

29. Sun C, Shi VG. PhysiNet: A combination of physics-based model and neural network model for digital twins. Int J Intell Syst. 2022; 37: 5443–5456. DOI: https://doi.org/10.1002/int.22798.

МЕТОД ПЕРЕВІРКИ ТОЧНОСТІ ОБЧИСЛЮВАЛЬНИХ РЕАЛІЗАЦІЙ ДЛЯ РОЗВ'ЯЗАННЯ ЗАДАЧ МОДЕЛЮВАННЯ ДИНАМІЧНИХ СИСТЕМ

Dr.Sci., Положаєнко С., Dr.Sci., Фомін О., Прокофьева Л., Ph.D., Прокофьев А., Ph.D., Савельев А., Філін Д.
Національний університет «Одеська політехніка», Україна,

Анотація. *Сучасні системи керування та моделювання значною мірою залежать від обчислювальних ресурсів, що реалізують алгоритми для аналізу динамічних систем у режимі реального часу. Це робить розробку компактних та ефективних алгоритмічних засобів самоконтролю нагальною потребою. Метою даної роботи є підвищення якості та надійності моніторингу обчислювального процесу чисельного розв'язання динамічних рівнянь шляхом застосування допоміжних алгоритмічних процедур, які виконуються паралельно з основним алгоритмом, але мають меншу обчислювальну складність. Основні завдання: розробити та обґрунтувати критерії виявлення помилок і збоїв у роботі основного обчислювального алгоритму; створити метод прийняття рішення щодо продовження обчислювального процесу після виявлення розбіжностей; сформулювати та перевірити метод інтерполяції для моніторингу точності в режимі реального часу на кроці інтегрування. У цій роботі запропоновано комбінований підхід, що включає метод із підвищенням обчислювальної точності: на кожному кроці інтегрування апроксимації функції стану визначаються послідовно зі зростаючим порядком точності для локальної похибки. Використання попередньо обчислених похідних на проміжних етапах усуває необхідність перерахунку обчислювально-містких правих частин системи, тим самим зменшуючи ризик збою. Точність контролюється опосередковано шляхом порівняння еталонного значення з результатом допоміжної формули. Результати та практичне значення: інтерполяція*

Ключові слова. *Динамічні системи, обчислювальна точність, чисельні розв'язки, методи керування на основі інтерполяції, верифікація математичних моделей, виявлення несправностей, прийняття рішень.*

UDC 004.05
DOI

METHODOLOGICAL FRAMEWORK FOR PERFORMANCE TESTING AND EVALUATION OF RESTFUL API USING AUTOMATED TESTING TOOLS

Ph.D. Khlamov S. [0000-0001-9434-1081], Mendielieva M. [0009-0002-4282-3147],
Ph.D. Vovk O. [0000-0001-9072-1634], Trunova T. [0000-0003-2689-2679],
Ph.D. Deineko Zh. [0000-0003-0175-4181], Lytvynenko S. [0009-0003-2632-9082]
Kharkiv National University of Radio Electronics, Ukraine
EMAIL: sergii.khlamov@gmail.com

Abstract. *The performance of REST API load-testing tools varies depending on workload characteristics, testing objectives, and infrastructure constraints. This study compares k6, Apache JMeter, and Postman under a controlled and unified REST API testing environment using consistent workloads and multiple load profiles. Performance and resource utilization were measured to identify differences in tool behavior and practical trade-offs. The results show that the evaluated tools have distinct performance profiles and that no single tool is optimal across all testing scenarios. SWOT analysis was used to summarize the experimental findings and identify key tool characteristics. Based on these results, a scenario-based approach was developed for four testing scenarios: latency critical, CPU constrained, memory constrained, and stress testing. The study demonstrates that load-testing tool selection should be based on the primary objective and constraints of a specific testing scenario.*

Keywords: *REST API, load testing, performance testing, resource utilization, load-testing tools, tool selection, scenario-based selection.*

Introduction

Performance testing is essential for assessing whether software systems can sustain realistic workloads and meet performance requirements [1]. Its importance has increased with the widespread of microservices, cloud platforms, and DevOps (Development and Operations), where REST (Representational State Transfer) APIs (Application Programming Interfaces) play a central role in distributed system interactions [2].

Numerous open-source and commercial tools are available for REST API load testing, differing in workload generation, scripting, resource consumption, reporting, and CI/CD (Continuous Integration/ Continuous Delivery) integration [3]. These differences can lead to different tool behavior across workload scenarios: a tool with favorable response-time performance may consume more computational resources or behave less predictably as the workload increases. The resulting research problem is to determine which load-testing tool is most appropriate for a given testing context, considering workload characteristics, REST API requirements, and infrastructure constraints. Although numerous studies have evaluated and compared performance testing tools [4], the existing literature largely focuses on specific tool combinations, individual testing scenarios, or isolated performance characteristics. Comparisons conducted under different experimental conditions also make it difficult to determine whether the observed differences are attributable to the testing tool itself, the workload profile, the characteristics of the tested API, or the underlying

infrastructure. This motivates the development of an experimentally grounded approach for scenario-specific REST API load-testing tool selection.

This monograph addresses this gap through a controlled comparison of k6, JMeter, and Postman tools using a unified REST API testing environment, consistent workloads, and multiple load profiles. The study analyzes their performance, resource utilization, and practical trade-offs to develop an approach to tool selection under different testing objectives and infrastructure constraints.

Literature review

Performance testing is essential for developing software products that meet user requirements. Web server performance directly affects the speed, efficiency, reliability, and overall user experience of web applications [3]. As demand for high-performance web services increases, evaluating web servers and applications under different workload conditions becomes increasingly important. However, scalability and maintenance challenges can limit the ability of web application architectures to satisfy growing performance and load-testing requirements, particularly in high-load environments [5]. Due to the time-consuming nature of performance testing, its integration into DevOps CI/CD pipelines has become important for accelerating software delivery and reducing testing delays [6]. Several open-source and widely used tools support web and API performance testing. Grafana k6 is an open-source load-testing tool developed in Go that combines high execution performance with ease of use and supports JavaScript-based test scripting [7, 8]. Its CLI-oriented (Command Line Interface) design, Docker support, and relatively low resource consumption make it suitable for automated and high-load testing scenarios [9, 10]. Apache JMeter is an open-source performance-testing tool supporting multiple protocols and workload configurations [11]. Apache JMeter architecture is based on the concept of emulated users. JMeter employs XML-based test plans with thread-based load generation. Test scenarios in JMeter are structured into Thread Groups, which define the number of concurrent users and the execution behavior of the workload Each emulated user is represented by a separate thread responsible for generating requests to the system under test according to the specified configuration. JMeter built-in components and extensions can be combined to define different workload patterns and reproduce complex testing scenarios. However, JMeter may exhibit high memory consumption during large-scale tests and has limitations related to real-time monitoring and the complexity of distributed test configuration [12, 13, 14]. Postman is a widely used API development and testing platform that also supports performance testing through predefined load profiles and automated JavaScript-based test scripts [15, 16, 17]. Its user-friendly interface and API-oriented workflow can simplify test development and monitoring, although limitations include resource-dependent virtual-user capacity, restricted test-data configuration, and limited support for introducing request delays in performance scenarios. Command-line execution is another important characteristic of performance-testing tools because it simplifies automated, repeatable, and CI/CD-integrated testing. CLI-based execution allows test configurations and runtime parameters to be explicitly defined and version-controlled while avoiding the additional resource overhead associated with graphical interfaces. Apache JMeter provides a dedicated command-line mode for load testing, while k6 is primarily designed around CLI-based execution. Postman

also supports automated execution through the Postman CLI, enabling collections and performance tests to be integrated into CI/CD workflows [18]. Previous studies have compared performance-testing tools under different workloads and testing environments. Study [4] evaluated Apache JMeter, Grafana k6, Gatling, Locust, and Artillery in a Jenkins-based CI/CD pipeline using representative, maximum, and spike workloads. Grafana k6 demonstrated the highest resource efficiency across the evaluated scenarios. A comparative study [19] of JMeter, k6, Gatling, and Locust using web-game workloads showed that tool performance depends strongly on workload characteristics: k6 performed best in write-intensive scenarios, JMeter in read-intensive workloads, Gatling provided efficient memory utilization under mixed loads, and Locust was suitable for resource-constrained environments. Other research reported that Postman achieved higher overall performance than JMeter and Robot Framework [20], while a comparison of Karate DSL, REST Assured, k6, and JMeter showed differences in test execution time, with JMeter requiring the longest execution time in the evaluated scenarios [3].

Overall, existing studies confirm the importance of performance testing and demonstrate substantial differences between testing tools. However, variations in testing environments, workloads, and evaluation criteria make their results difficult to use as a direct basis for tool selection. Existing research often evaluates tools according to general performance characteristics rather than considering specific workload profiles, API requirements, and infrastructure constraints.

Controlled experiments using a common environment and consistent workloads can provide a more comparable basis for evaluation. Therefore, this monograph combines controlled experimental evaluation with systematic analysis of tool characteristics. SWOT analysis is used to interpret the experimental findings, which are subsequently applied to develop a scenario-based approach for selecting REST API load-testing tools according to the primary objective and constraints of each testing scenario.

Methodology

The experimental methodology was used to compare the performance of three load testing tools under different workload patterns. The experimental environment was deployed on a local physical server to minimize the influence of network latency and external infrastructure variability. All experiments were executed under identical hardware and software conditions to ensure reproducibility and fair comparison between the evaluated load testing tools. Experiments were conducted on a workstation equipped with Windows 11 x64 25H2, equipped with an Intel Core i9-11900H 8-core CPU and 16 GB RAM. The application under test was implemented as a RESTful API using Node.js with the Express framework. Data persistence was provided by the Better-SQLite3 embedded database. Synthetic test data were generated using the Faker library to create realistic datasets while maintaining identical input conditions across test runs (Figure 1a). The supporting services were executed in Docker containers (see Figure 1b). Resource utilization were collected using Prometheus, while Grafana was used for visualization and inspection of CPU and memory (RAM) consumption throughout each experiment.

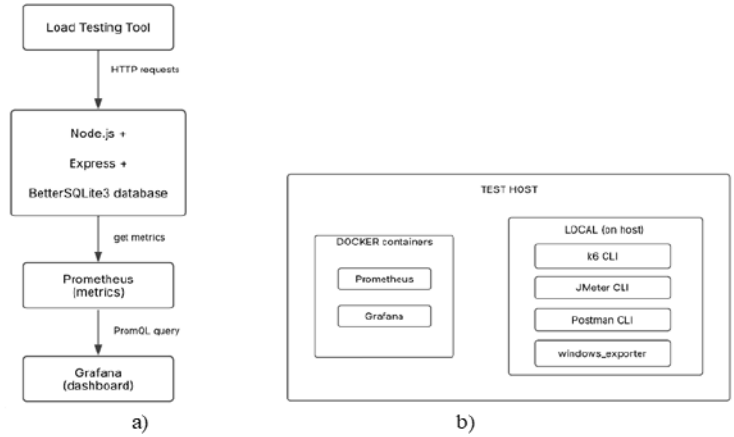


Figure 1. Experimental environment: a) architecture; b) supporting services (source: own elaboration)

The supporting services were executed in Docker containers (see Figure 1b). Resource utilization were collected using Prometheus, while Grafana was used for visualization and inspection of CPU and memory (RAM) consumption throughout each experiment. To ensure consistency, the same application version, database state, workload configuration, and monitoring setup were used for every experimental run. Each Tool × Load combination was executed 10 times under identical conditions: Node.js – v24.16.0; Express – v5.2.1; Better-SQLite3 – v12.11.1; Faker – v5.5.3; Docker – v4.81.0; Prometheus – v3.12.0; Grafana – v13.0.2. The application uses a relational database consisting of four entities: Users, Products, Orders, and Order_Items, as shown in entity-relationship (ER) diagram on Figure 2. Each user could create multiple orders, and each order contained one or more order items linked to products, representing a simplified e-commerce workflow for CRUD performance evaluation. A Better-SQLite3 database was populated with 1000 users, 3000 products, 10000 orders, and 30000 order items. Before each experiment, the database was restored from a predefined dump and the local application server was restarted to ensure identical initial conditions.

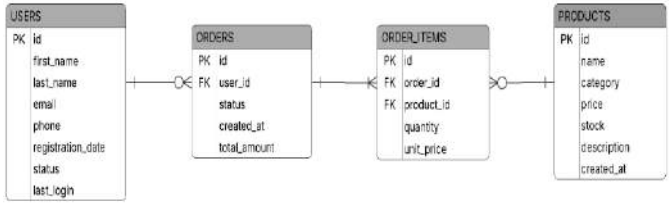


Figure 2. ER diagram of the experimental database schema (source: own elaboration)

Four workload profiles were designed to represent common performance testing scenarios: Ramp, Spike, Peak, and Fixed. Each workload profile was executed independently using all three load testing tools. For every Tool × Load combination,

10 independent experimental runs were performed to reduce the influence of random variation. Each load profile defines a different pattern of virtual user generation over time. The workload patterns used in this study are illustrated in Figure 3.

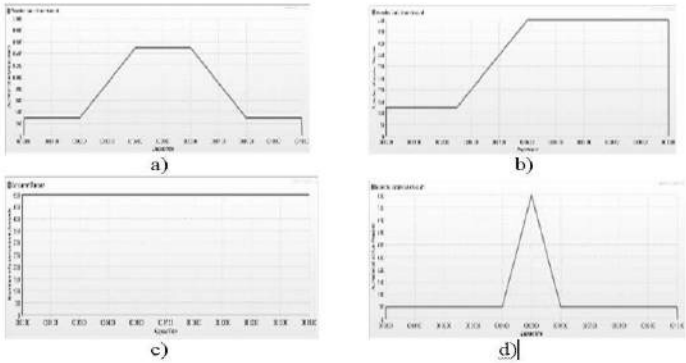


Figure 3. Load type visualization: a) Ramp; b) Spike; c) Peak; d) Fixed. (source: own elaboration)

A common logical test scenario was implemented in k6, Apache JMeter, and Postman for cross-tool comparison. Although the tools use different workload-generation mechanisms, equivalent configurations were selected to reproduce the same workload profiles (e.g., ramping-vus and constant-vus in k6, Ultimate and Concurrent Thread Groups in JMeter, and predefined load profiles in Postman). The endpoint sequence, test conditions, and iteration data selection strategy were kept consistent across all experiments. The configurations are summarized in Table 1.



Figure 4. HTTP requests used in test plan/collection for JMeter and Postman (source: own elaboration)

To ensure realistic and comparable workload generation, the scenario included product and order operations (Figure 4), multi-table database joins, and data aggregation. A fixed 3 second think time was applied between requests across all tools, using the Constant Timer in JMeter, the Postman Echo delay endpoint in Postman, and sleep() in k6.

Table 1

Workload configurations

Workload profile	Tool	Test Duration, min	Configuration
Ramping load	K6	10	ramping-vus; startVUs=125; stages: 125→500 (5 min), 500→500 (5 min)
	JMeter	10	Ultimate Thread Group: 1) start threads count = 125, initial delay =0, startup time = 0, hold load for = 600 s, shutdown time = 0 s 2) start threads count = 325, initial delay = 150 s, startup time = 150 s, hold load for = 300 s, shutdown time = 0 s
	Postman	10	Ramp-up load profile; initial load = 125, Virtual users = 500, Test duration = 10 min
Spike load	K6	10	ramping-vus; startVUs: 80; stages: 80 (4 min), 80→800 (1 min), 800→80 (1 min), 80 (4 min)
	JMeter	10	Ultimate Thread Group: 1) start threads count = 80, initial delay =0, startup time = 0, hold load for = 600 s, shutdown time = 0 s 2) start threads count = 720, initial delay = 240 s, startup time = 60 s, hold load for = 0 s, shutdown time = 60 s
	Postman	10	Spike load profile; initial load = 80, Virtual users = 800, Test duration = 10 min
Peak load	K6	10	ramping-vus; startVUs: 300; stages: 300 (2 min), 300→1500 (2 min), 1500 (2 min), 1500→300 (2 min), 300 (2 min)
	JMeter	10	Ultimate Thread Group: 1) start threads count = 300, initial delay =0, startup time = 0, hold load for = 600 s, shutdown time = 0 s 2) start threads count = 1200, initial delay = 120 s, startup time = 120 s, hold load for = 120 s, shutdown time = 120 s
	Postman	10	Peak load profile; initial load = 300, Virtual users = 1500, Test duration = 10 min
Fixed load	K6	15	constant-vus; vus: 500; duration: 15m
	JMeter	15	Concurrency Thread Group: target concurrency = 500, hold target rate = 15 min
	Postman	15	Fixed load profile; virtual users = 500, Test duration = 15 min

```
  //GET PRODUCTS
  const getProd = http.get("http://localhost:8080/api/products", {
  tags: {
    endpoint: "GET /products"
  }
});
  sleep(3);
  check(getProd, {'products are read successfully': r => r.status === 200});

  //GET ORDERS
  const getOrders = http.get("http://localhost:8080/api/orders", {
```

```
  tags: {
    endpoint: "GET /orders"
  }
});
  sleep(3);
  check(getOrders, {'orders are read successfully': r => r.status === 200});

  //GET ORDER DETAILS
                                    const                    getOrderDetails                    =
http.get(`http://localhost:8080/api/orders/${orderIdGet}/details`, {
  tags: {
    endpoint: "GET /orders/:id/details"}
});
  sleep(3);
  check(getOrderDetails, {'order details are read successfully': r => r.status === 200});

  //POST - CREATE ORDER
  const createRes = http.post(http://localhost:8080/api/orders',payload,
    {
      headers: {
        'Content-Type': 'application/json'
      },
      tags: {
    endpoint: "POST /orders"}
    },
  );
  sleep(3);

  check(createRes, {
    'order created': r => r.status === 201
  });
  const createdOrder = createRes.json();
  const orderId = createdOrder.orderId;
```

Listing 1. Example of part of HTTP requests sequence used in k6 test scenario

Predefined test data were selected deterministically using the iteration index (__ITER in k6 and equivalent iteration variables in JMeter and Postman) as shown in Listing 2 and Figure 5. Five values were cycled for userId, productId, and orderId to distribute database access and avoid repeatedly targeting the same records [21].

```
const users = [1, 2, 3, 4, 5];
const products = [10, 20, 30, 40, 50];
const orders = [10, 20, 30, 40, 50];

function pick(arr, index) {
  return arr[index % arr.length];
}

//flow logic
export default function() {
  const userId = pick(users, __ITER);
    const productId1 = pick(products,
__ITER);
```

```
def users = [1, 2, 3, 4, 5]
def products = [10, 20, 30, 40, 50]

def threadNum = ctx.getThreadNum()

Integer iteration = vars.getObject("iteration")
if (iteration == null) {
 iteration = 0
}

vars.putObject("iteration", iteration + 1)

int index = threadNum + iteration
```

```
   const productId2 = Number(productId1
+ 1);
      const orderIdGet = pick(orders,
__ITER);

   // PAYLOAD - CREATE ORDER
   const payload = JSON.stringify({
      userId: userId,
      status: "NEW",
      items: [
         {
            productId: productId1,
            quantity: 1
         },
         {
            productId: productId2,
            quantity: 2
         }
      ]
   });
```

a)

```
log.info("iteration = " + vars.get("iteration"))

int productId1 = products[index %
products.size()]
int productId2 = productId1 + 1

vars.put("userId", users[index %
users.size()].toString())
vars.put("productId1",
productId1.toString())
vars.put("productId2",
productId2.toString())
```

b)

Listing 2. Selection of test identifiers in: a) k6; b) JMeter JSR223 POST preProcessor

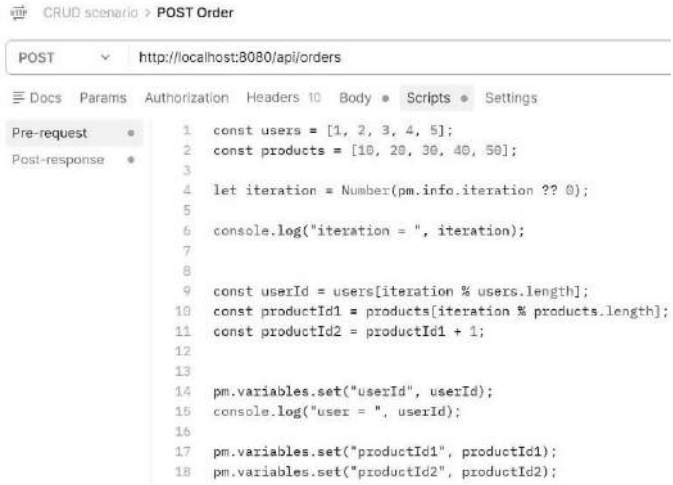


Figure 5. Selection of test identifiers in Postman pre-request script for POST request (source: own elaboration)

To ensure a fair comparison across all evaluated tools, the workload profiles were designed according to the load generation strategies supported by all platforms. In particular, the four workload profiles (Ramp, Spike, Peak, and Fixed) were adopted because they are natively supported by Postman and can be equivalently implemented in k6 and JMeter.

All experiments were executed through the CLI of each evaluated tool to ensure a consistent and reproducible execution procedure. CLI-based execution was used to provide a consistent and reproducible test procedure and to minimize the influence of interactive configuration during test execution. Tool-specific CLI commands were used to initialize the tests, configure the required workload parameters, and export the execution results for subsequent analysis. The example of commands for k6, JMeter, and Postman is provided below:

```
k6 run test-ramp-load.js --summary-export=ramp_run_1.json --out json=ramp_out_1.json

.\jmeter -n -t "D:\Ramp_Ultimate_Thread_Group_mixed.jmx" -l D:\ramp_run_1.jtl

postman login --with-api-key {api_key}
postman performance run {collection_id} --vu-count 500 --duration 10 --load-profile ramp-up
```

Metrics and statistical analysis

During each experimental run, performance metrics (average response time, 95th percentile (p95) response time, CPU utilization, and RAM consumption) together with workload execution metrics (total requests and completed iterations) and error metrics (overall error rate, HTTP errors, connection errors, and request timeouts) were recorded. The analysis was based on 10 independent runs for every Tool × Load combination. Response time metrics characterize both the typical request latency and its variability under different workload conditions, while resource utilization metrics (CPU and RAM) reflect the computational overhead introduced by each tool. To ensure consistent comparison across the evaluated tools, Postman JSONError events were classified as HTTP errors because they represent failures in client-side processing of successfully received HTTP responses rather than connection failures or request timeouts.

Since each experimental run included multiple REST API endpoints with different response times, a single performance value was calculated for every Tool × Load × Run combination. Specifically, the Metric Mean Response Time (M) was calculated as the arithmetic mean of the average response times measured for all evaluated endpoints:

$$M = \frac{1}{N} \sum_{i=1}^{N} R_i , \quad (1)$$

where R_i - denotes the average metric value of the i-th endpoint during a single experimental run; N - is the total number of evaluated endpoints.

Average response time (Avg) was used to evaluate typical system latency, while the p95 metric was analyzed to capture tail latency and identify performance degradation under load. CPU and RAM utilization were monitored on the local host using Prometheus time-series data in Grafana while executing the load tests (see Figure 6 and Figure 7). CPU and RAM utilization reported in this study represent only the resource consumption of the load-testing tool processes (k6, Apache JMeter, and Postman). Host-wide CPU and memory utilization were intentionally excluded from the analysis. Process-level metrics were collected using windows_exporter and retrieved from Prometheus via PromQL queries filtered by the process name (process="k6", process="java", process=~"postman"). During the experiments, no

other Java processes except Apache JMeter were running on the load-generation host. For both CPU and memory metrics, values were aggregated by summing all matching process instances. CPU usage was calculated from the windows_process_cpu_time_total metric using the PromQL function rate(), while memory consumption was obtained from windows_process_working_set_bytes.

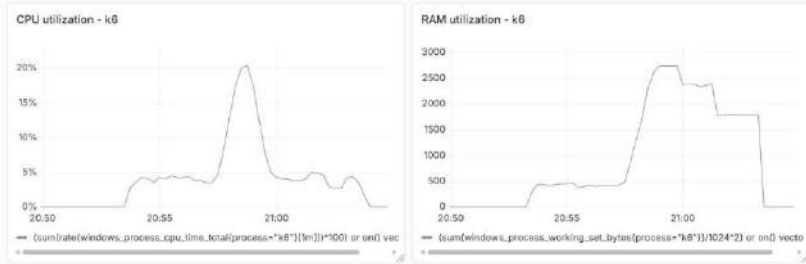
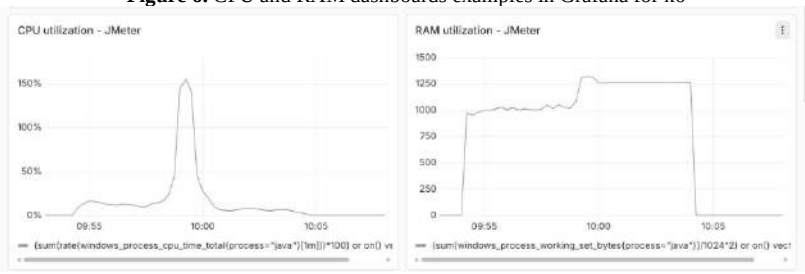
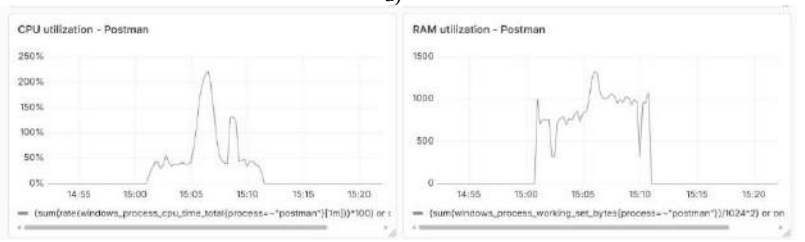


Figure 6. CPU and RAM dashboards examples in Grafana for k6



a)



b)

Figure 7. CPU and RAM dashboards examples in Grafana: a) Jmeter; b) Postman

The collected metrics served as dependent variables in the subsequent statistical analysis. Each experimental run provided raw response time and resource utilization measurements. These metrics were collected during a test run and aggregated into a single value. For statistical analysis, each row in resulting dataset represented an aggregated observation. For overall performance metrics, an observation corresponded to a Tool-Load-Run combination, while endpoint-level observations additionally included the API endpoint identifier. Average response time, p95 response time and errors were obtained directly from the summary reports exported by k6, JMeter, and Postman for each experimental run. Endpoint-level response time

metrics were extracted from the corresponding endpoint-level reports and analyzed separately by applying the same statistical procedure to each endpoint individually. For k6 endpoint-level performance metrics were obtained by post-processing the exported JSON test report with a custom Python script, which aggregated HTTP request measurements by endpoint using only http_req_duration records and calculated the corresponding response time (avg, p95) statistics. CPU and RAM utilization were obtained from Prometheus time-series data in Grafana by first aggregating all matching process instances and then calculating the arithmetic mean of the sampled values over the test duration using the Grafana Mean function on Stat panel of the created test dashboard. Experimental results were exported after each execution and processed using Python.

Scenario-Based Approach for Tool Selection

The SWOT analysis was used to develop a scenario-based approach for REST API performance tool selection under different testing objectives and infrastructure constraints. The approach selects a preferred tool for each testing scenario based on the primary criterion associated with the scenario's main testing objective (Figure 8).

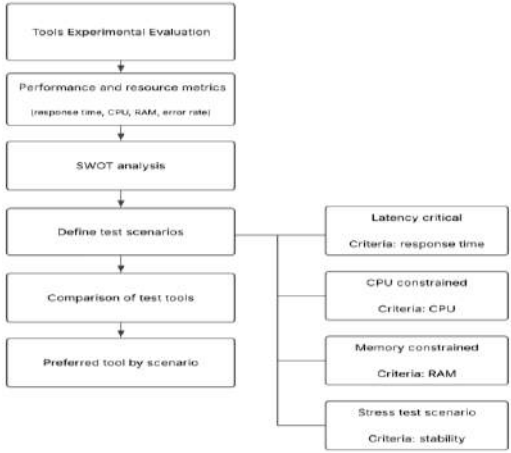


Figure 8. Scenario-Based Approach for Tool Selection

Four representative testing scenarios were defined based on the identified performance characteristics, resource constraints, and practical implications of the SWOT analysis: latency critical testing, CPU constrained testing, memory constrained testing, and stress testing under increasing workload. Each scenario represents a distinct testing objective or infrastructure constraint and therefore prioritizes a different performance characteristic. For the latency critical scenario, response time is the primary criterion. For CPU and memory constrained scenarios, CPU and memory consumption are used as the respective primary criteria. For stress testing, the primary criterion is operational stability under increasing workload. In this study, operational stability refers to the ability of a testing tool to maintain consistent operation and predictable performance as the workload increases without

critical failures. Stability is assessed based on changes in response time, resource consumption, and error rate across increasing workload levels.

For each testing scenario, the relevant performance and resource criteria are first identified according to the primary testing objective. The evaluated tools are compared directly with respect to the criterion (Table 2), and the tool with the most favorable result is identified as the preferred candidate.

Table 2

Scenario-based selection

Scenario	Testing Objective	Criterion
Latency critical	Minimize response time	Avg and p95 response time
CPU constrained	Minimize CPU consumption while maintaining competitive avg or p95	CPU utilization
Memory constrained	Minimize memory consumption while maintaining competitive avg or p95	Memory utilization
Stress testing	Maintain stable operation under increasing workload	Stability, error rate

Results

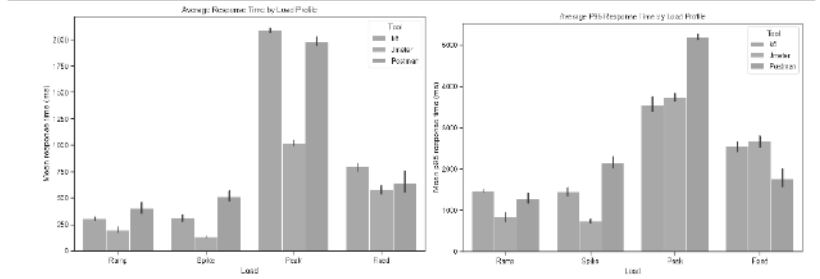
To provide an initial comparison of the evaluated performance testing tools, the average response time (avg) for each workload level and then standard deviation, and 95% confidence interval (95% CI) were calculated. These descriptive statistics summarize the overall behavior of each tool before applying statistical analysis (Table 3).

Table 3

Aggregated Average response time performance metric values

Tool	Load	Mean Avg	Standard Deviation	95% CI lower	95% CI upper	Error Rate
k6	Ramp	305.338	18.502	292.1027	318.573	0
JMeter	Ramp	194.6	45.998	161.695	227.505	0
Postman	Ramp	400.6	89.641	336.475	464.726	0.0302
k6	Spike	312.15	48.403	277.524	346.776	0.0003
JMeter	Spike	132.3	8.460	126.248	138.352	0.017
Postman	Spike	510.383	79.221	453.712	567.054	0.4052
k6	Peak	2090.722	32.580	2067.416	2114.028	15.229
JMeter	Peak	1022.1	38.869	994.295	1049.905	14.5583
Postman	Peak	1984.733	62.897	1939.74	2029.727	13.4913
k6	Fixed	794.197	63.273	748.934	839.460	0.246
JMeter	Fixed	575.6	60.959	531.992	619.208	0.7538
Postman	Fixed	637.4	166.239	518.480	756.321	1.3898

The results in Table 3 and Figure 9a presents the aggregated average response time (avg) for the evaluated performance testing tools under different load profiles. Error bars correspond to the 95% confidence interval. The results show that k6 demonstrated the highest average response time across Peak and Fixed load, while JMeter had the lowest response time across all tested load types. Postman showed higher response time for Ramp and Spike load.

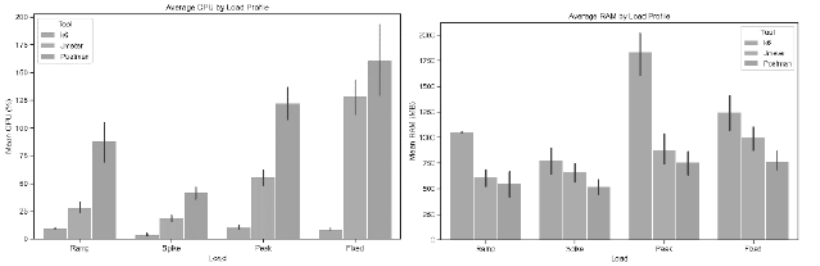


a) b)

Figure 9. Mean response time: a) Average; b) p95 response time (source: own elaboration)

Figure 9b demonstrates the aggregated p95 response time for evaluated performance testing tools under 4 workload profiles. For the Ramp and Spike workload profiles, JMeter tool consistently demonstrates lower p95 values than the other tools. The differences between p95 values of k6 and JMteter are relatively small for the Fixed profile, but become more pronounced under Peak loads for Avg metric. Postman p95 value increases more than the others for the Spike and Peak profiles, but for the Fixed profile, it is the smallest of all test tools.

K6 tool demonstrated lower CPU utilization but higher memory consumption compared with the other tools, as shown in Figure 10a. This indicates a different resource utilization pattern during workload generation by tools. In addition to higher RAM consumption (Figure 10b), k6 had a higher average response time than JMeter. This suggests that JMeter was a more resource-efficient under the evaluated conditions. Postman had the highest CPU utilization during all load types in CLI mode, but lower RAM consumption than JMeter and k6.



a) b)

Figure 10. Average resources consumption by Load profile: a) CPU; b) RAM (source: own elaboration)

Figure 11 and Figure 12 present average and p95 response times across endpoints and workload profiles. Colors denote evaluated tools, and error bars represent 95% confidence intervals. and endpoint-level analysis confirmed that tool performance depends on request type and workload profile. JMeter provided the most stable performance for both read and write operations, while k6 showed increased latency for complex GET requests under Peak load. Postman achieved competitive results only for specific retrieval scenarios under Fixed workload.

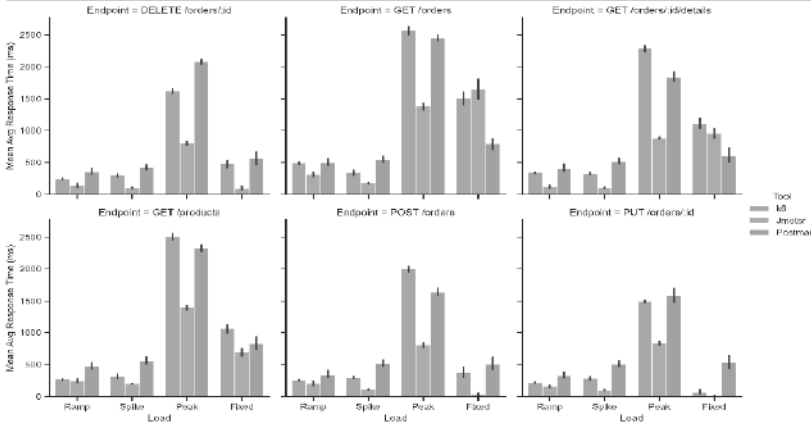


Figure 11. Mean Avg response time across endpoints (source: own elaboration)

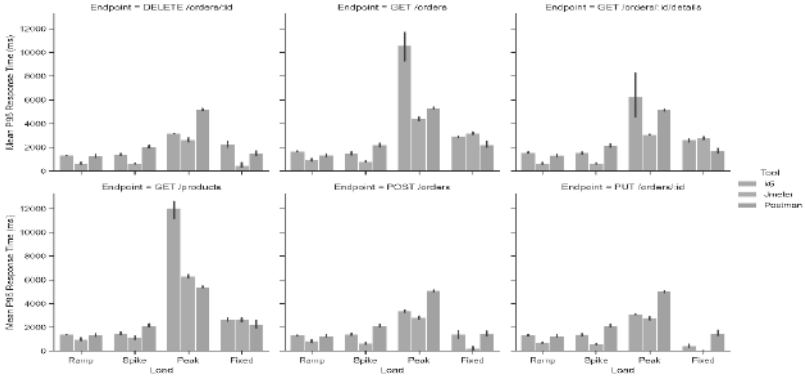


Figure 12. Mean p95 response time across endpoints (source: own elaboration).

To summarize the experimental findings and their practical implications, a SWOT analysis was performed for the evaluated performance testing tools. The analysis summarizes the principal strengths and weaknesses identified from the experimental results and relates them to potential application scenarios. Opportunities represent potential use cases derived from the observed characteristics of each tool, whereas threats reflect contextual conditions that may limit the applicability of these characteristics. Execution environment sensitivity in Table 4 refers to the potential dependence of measured performance on hardware, software, and runtime conditions. Then, based on SWOT matrix the comparative analysis was performed by considering both performance and resource-related criteria across the evaluated workload profiles. Average and p95 response times were interpreted using a lower-is-better direction, whereas stability was evaluated using a higher-is-better direction (or using the lower-is-better direction for error rate).

Table 4

SWOT matrix

	JMeter	K6	Postman
Strengths	Low latency	CPU efficiency	Efficient in read operations for Fixed load
Weaknesses	Higher CPU consumption	Higher RAM consumption	Higher latency for write operations
Opportunities	Sutable for latency-sensitive testing scenarios	Suitable for Resource-constrained testing	Suitable for lightweight testing
Threats	Sensitivity to execution environment	Memory constraints	Potentially insufficient for high-load scenarios

CPU utilization and RAM consumption were also interpreted according to the lower-is-better principle. For latency-critical testing, JMeter demonstrated the best response-time characteristics across most workload profiles, while k6 and Postman showed higher latency under specific high-load conditions. JMeter provided the most stable performance for both read and write operations, while k6 showed increased latency for complex GET requests under Peak load. Postman achieved competitive results only for read Fixed load. Regarding CPU constrained environments, k6 provides the smallest overall CPU consumption. Additionally, Postman and JMeter can be potentially applied in memory constrained test scenarios. Moreover, Postman tool can be considered the most suitable candidate for lightweight testing, where low memory consumption and ease of use are more important than CPU efficiency, for example in moderate-load test runs with simple API. k6 and JMeter can be suitable for stress testing scenario because they maintain stable operation under increasing workload levels, despite not providing the lowest resource consumption.

Conclusions

In conclusion, this monograph presented an approach to selecting REST API load-testing tools under different testing objectives and infrastructure constraints. K6, JMeter, Postman test tools were evaluated under consistent testing conditions and multiple workload profiles with respect to response time, CPU and memory utilization, and performance stability under increasing workload. The findings showed that the evaluated tools have different performance and resource profiles, making a universal ranking inappropriate. SWOT analysis was used to synthesize these differences and identify the characteristics relevant to practical tool selection. Based on the SWOT findings, a scenario-based approach was developed in which a criterion is assigned to each testing objective. Four scenarios were considered as latency critical, CPU constrained, memory constrained, and stress testing. The resulting recommendations show that JMeter might be preferable for latency-critical and stress-testing scenarios, k6 for CPU-constrained environments, and Postman for lightweight testing with moderate load. Thus, the study demonstrates that load-testing tool selection can be treated as a context-dependent decision based on the primary objective of the testing scenario rather than on a universal performance ranking. The proposed approach provides a structured basis for translating experimental measurements into practical tool-selection recommendations. Its applicability is

limited by the evaluated tools, experimental environment, and workload profiles, which provides opportunities for further validation across additional tools, APIs, workload patterns, and infrastructure configurations.

References

[1] Binder, E., Li, X., & Janes, A. (2026). An Agent-Based Approach to Automating Software Performance Testing (Work In Progress Paper). *In Companion of the 17th ACM/SPEC International Conference on Performance Engineering*. (pp. 55-61). https://doi.org/10.1145/3777911.3801107.

[2] Peldszus, S., Rutenkolk, J., Heide, M., Sollmann, J., Klatt, B., Köhne, F., & Berger, T. (2026). Developer Perspectives on REST API Usability: A Study of REST API Guidelines. *In Proceedings of the 34th ACM International Conference on the Foundations of Software Engineering*. (pp. 966-977). https://doi.org/10.1145/3803437.3805267.

[3] Shah, Y. R. Comparative Analysis of API Test Automation Frameworks: An Experimental Study on Performance, Reliability, and CI/CD (Computer science), Ph.D. thesis, Parul University, Vadodara, Gujarat, India, 2026.

[4] Pinyagin, M., & Sadovykh, A. (2026). Automating Performance Testing in CI/CD - Tools Evaluation. In: Bonfanti, S., Papadopoulos, G.A. (eds). *Testing Software and Systems. ICTSS 2025. Lecture Notes in Computer Science*, 2025, vol 16107. Springer, Cham. https://doi.org/10.1007/978-3-032-05188-2_13.

[5] Chaudhary, P., & Banerjee, D. (2024). Continuous Performance Assurance in Cloud-Native Environments: A Testing Framework for Microservices and Serverless Architectures. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, 7(6), 11289-11302, https://doi.org/10.15662/ IJARCST. 2024.0706014.

[6] Henning, S., & Hasselbring, W. (2022). A configurable method for benchmarking scalability of cloud-native applications. *Empirical Software Engineering*, 27(6), 143.

[7] Di Meglio, S., & Starace, L. L. L. (2024). Evaluating performance and resource consumption of rest frameworks and execution environments: Insights and guidelines for developers and companies. *IEEE Access*, 12, 161649-161669. https://doi.org/10.1109/ ACCESS.2024.3489892.

[8] Kravchenko, Y., Leshchenko, O., Trush, O., Dakhno, N., & Krasnopyorov, P. (2023). Optimizing and Improvement a Web Application Using Open Source Tools. *In IT&I*. (pp. 368-379).

[9] Hegyi, G. I., Maliosz, M., & Simon, C. (2019). Performance measurements of function as a service platforms. *In Proceedings of the 2019 3rd International Symposium on Computer Science and Intelligent Control*. (pp. 1-6).

[10] Pinastawa, I. W. R., Pradana, M. G., & Maulana, N. (2024). Web server performance evaluation: Comparing nginx and apache using k6 testing methods for load, spike, soak, and performance. *In 2024 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*. (pp. 1002-1007). IEEE.

[11] Leonov, S., & Tyrtyshnyi, D. (2026). Performance Optimisation of real-time data ingestion: Enhancing the InfluxDB backend listener for Jmeter. *Вісник Національного технічного університету "ХПІ". Серія: Інформатика і моделювання*, 1(15), 43-67. https://doi.org/10.20998/2411-0558.2026.01.03.

[12] Gupta, V. K., Gupta, A., Jain, P., Singh, S., & Singh, L. K. (2025). Enhancing Productivity in Software Testing Automation: A Comparative Study of Open-Source Tools for Smart Manufacturing. *In 2025 2nd Global AI Summit-International Conference on Artificial Intelligence and Emerging Technology (AI Summit)*. (pp. 1307-1312). IEEE.

[13] AutomateNow. (2023). Advantages and Disadvantages of using JMeter. https://automatenow.io/advantages-and-disadvantages-of-using-jmeter/.

[14] TestSigma. (2025). JMeter vs Postman. https://testsigma.com/blog/jmeter-vs-postman/.

[15] Sapundzhi, F., Jovanova, E., Popstoilov, M., Georgiev, S., Georgiev, I., Stefanova, T., & Todorov, V. (2025). An Integrated Approach to Evaluating E-Commerce Platforms using Postman and Selenium. *In 2025 6th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*. (pp. 1-6). IEEE.

[16] Postman. (2026). Performance Test Configuration. https://learning.postman.com/docs/tests-and scripts/performance-testing/performance-test-configuration.

[17] Patil, G. (2025). Postman. *In: Django REST APIs Demystified. Apress, Berkeley, CA*. https://doi.org/10.1007/979-8-8688-1850-9_5.

[18] Thooriqoh, H. A., Mulyo, B. M., & Rakhmadi, A. (2024). Advanced RESTful API Testing: Leveraging Newman's Command-Line Capabilities with Postman Collections. *In 2024 IEEE 10th Information Technology International Seminar (ITIS)*. (pp. 188-193). IEEE.

[19] Park, D., Kim, J. H., & Sung, H. (2025). Performance and Resource Efficiency Analysis of Load Testing Tools for Web Game Workloads. *Journal of Computer Games and Contents*, 38(7), 16-26.

[20] Hsieh, C.-H. et al. (2021). Evaluation System for Software Testing Tools in Complex Data Environment. *2021 4th International Conference on Information Communication and Signal Processing (ICICSP)*, Shanghai, China. (pp. 604-609). https://doi.org/10.1109/ICICSP54369.2021.9611846.

[21] Di Meglio, S., Starace, L. L. L., Pontillo, V., Martins, L., Di Nucci, D., & Palomba, F. (2026). A Taxonomy of Bad Practices in Software Performance Testing: Insights from Gray Literature and Practitioner Validation. *ACM Transactions on Software Engineering and Methodology*. https://doi.org/10.1145/3821538.

МЕТОДОЛОГІЧНИЙ ФРЕЙМВОРК ДЛЯ ТЕСТУВАННЯ ПРОДУКТИВНОСТІ ТА ОЦІНКИ RESTFUL API З ВИКОРИСТАННЯМ АВТОМАТИЗОВАНИХ ІНСТРУМЕНТІВ ТЕСТУВАННЯ

Ph.D. Хламов С., Мендєлєва М., Ph.D. Вовк О., Трунова Т., Ph.D. Дейнеко Ж., Литвиненко С.

Харківський національний університет радіоелектроніки, Україна

Анотація. *Продуктивність інструментів для навантажувального тестування REST API залежить від характеристик робочого навантаження, цілей тестування та обмежень інфраструктури. У цьому дослідженні порівнюються k6, Apache JMeter та Postman у контрольованому та уніфікованому середовищі тестування REST API з використанням узгоджених робочих навантажень та кількох профілів навантаження. Продуктивність та використання ресурсів вимірювалися для виявлення відмінностей у поведінці інструментів та практичних компромісів. Результати показують, що оцінювані інструменти мають різні профілі продуктивності, і що жоден інструмент не є оптимальним для всіх сценаріїв тестування. SWOT-аналіз було використано для узагальнення експериментальних результатів та визначення ключових характеристик інструментів. На основі цих результатів було розроблено сценарний підхід для чотирьох сценаріїв тестування: критична затримка, умови обмеженого CPU, умови обмеженої пам'яті та стрес-тестування. Дослідження демонструє, що вибір інструменту для навантажувального тестування повинен базуватися на основній меті та обмеженнях конкретного сценарію тестування.*

Ключові слова: *REST API, навантажувальне тестування, тестування продуктивності, використання ресурсів, інструменти для навантажувального тестування, вибір інструментів, вибір на основі сценаріїв.*

УДК 519.23: 004.932.4
DOI

БАГАТОСТАДІЙНИЙ КОНВЕЄР ОБРОБКИ ЗОБРАЖЕНЬ КОРОТКОХВИЛЬОВОГО ІНФРАЧЕРВОНОГО ДІАПАЗОНУ

Бондар Є.[1][0009-0001-5309-0084], Кутвицький М.[1][0009-0005-7098-3908], Нетребін Ю.[1][0009-0001-8778-3241], Dr. Sci., Саваневич В.[1][0000-0001-8840-8278], Ph.D., Хламов С.[1][0000-0001-9434-1081], Dr. Sci., Зеленський С.[2][0000-0001-8545-6784], Ph.D., Хорошевська І.[3][0000-0001-8990-9891], Ph.D., Табакова І.[1][0000-0001-6629-4927]

[1] Харківський національний університет радіоелектроніки, Україна,
[2] Київський національний університет імені Тараса Шевченка, Україна,
[3] Харківський національний економічний університет імені Семена Кузнеця, Україна

EMAIL: sergii.khlamov@gmail.com

Анотація. *Виявлення малорозмірних рухомих об'єктів у послідовностях зображень короткохвильового інфрачервоного діапазону (SWIR) потребує узгодження якості виявлення, координатної точності та швидкодії за неоднорідного й часозмінного фону. Розроблено багатостадійний конвеєр обробки від підготовки даних до формування вимірювань. На натурних і модельних даних досліджено вплив програмного бінування, способів та порядку обробки фону і масштабу ядра узгодженої фільтрації. Встановлено, що підвищення швидкодії завдяки бінуванню може супроводжуватися погіршенням координатної точності та якості виявлення. Ефективність обробки фону залежить від умов спостереження й порядку процедур, а раціональний масштаб фільтра залежить від розміру зображення об'єкта після бінування. Парето-аналіз виконано окремо для кожного з 12 наборів даних. Урахування практичної нечутливості до малих змін координатної похибки скоротило загальну кількість недомінованих конфігурацій із 40 до 25 раціональних альтернатив. Універсальної оптимальної конфігурації не встановлено. Результати забезпечують вибір параметрів конвеєра відповідно до умов спостереження та вимог до виявлення, точності й швидкодії.*

Ключові слова: *SWIR-зображення, багатостадійна обробка, програмне бінування, узгоджена фільтрація, Парето-оптимальність, критерій виявлення, координатна точність.*

Вступ

Виявлення малорозмірних слабкоконтрастних рухомих об'єктів ускладнюють шуми, неоднорідність і часова мінливість фону, особливо за значної дальності [1]. Їхні зображення можуть займати лише кілька пікселів, тому потрібне узгодження якості виявлення, координатної точності та швидкодії обробки. У короткохвильовому інфрачервоному діапазоні (SWIR) більша, ніж у видимому діапазоні, довжина хвилі створює передумови для меншого атмосферного розсіювання [2], однак пропускання залежить від спектральних вікон і поглинання водяною парою [3]. За денного пасивного спостереження переважає відбите сонячне випромінювання [4], а спектральні відмінності матеріалів можуть підвищувати контраст об'єкта відносно фону [5, 6]. Це обґрунтовує дослідження SWIR-систем виявлення [7] для оптико-електронного спостереження. Метою роботи є розробка багатостадійного конвеєра обробки послідовностей SWIR-зображень малорозмірних рухомих об'єктів, дослідження впливу програмного бінування, обробки фону та узгодженої фільтрації на якість виявлення, координатну точність і швидкодію та визначення раціональних конфігурацій за сукупністю цих показників.

Аналіз літературних даних

Підходи до виявлення об’єктів відрізняються ступенем декомпозиції обробки. Класифікація [8] розділяє перетворення зображення та критерій виявлення; огляди інфрачервоних методів охоплюють різні варіанти такої побудови [9, 10]. Для складного фону застосовують трансформери, орієнтовані на його структуру [11], гібридні мережі з просторовим і частотним аналізом [12] та пірамідальне об’єднання ознак із механізмами уваги [13]. Модульну обробку використовують і в системах комп’ютерного бачення для великих масивів кадрів [14]. Узгоджена фільтрація є перетворенням зображення, після якого застосовують окремий критерій виявлення [15]. Згортка з профілем очікуваного об’єкта підсилює його відносно фону та шуму. У задачах виявлення слабких джерел використовують послідовність оцінювання або віднімання фону, фільтрації на основі функції відгуку точки (PRF) та порогової обробки [16]. Послідовну декомпозицію ілюструє метод [17]: поділ на підобласті, перетворення зображення, адаптивне пригнічення шуму, пошарове виявлення та розділення злитих об’єктів. В інфрачервоних методах також виокремлюють пригнічення фонового шуму й усунення завад [18], зокрема поєднують віднімання фону методом змінних напрямків множників, удосконалене морфологічне top-hat-перетворення та адаптивну порогову сегментацію [19]. Подібні принципи послідовної обробки й розпізнавання рухомих об’єктів застосовано до великих масивів астрономічних даних [20]. Кінцевий результат залежить від параметрів бінування [21], способів вирівнювання яскравості та параметрів узгодженої фільтрації [22]. Міжкадрове й внутрішньокадрове вирівнювання фону можуть застосовуватися окремо або послідовно, тому значення має також порядок процедур. Для SWIR-спостереження актуальною є задача спільного оцінювання впливу цих рішень на якість виявлення, координатну точність і швидкодію. У роботі її вирішено шляхом експериментального дослідження багатостадійного конвеєра та багатокритеріального вибору його конфігурацій за процедурою оцінювання.

Матеріали та методи дослідження

Дослідження виконано на натурних SWIR-послідовностях, отриманих на стенді (рис. 1), та модельних даних. Варіювали програмне бінування, обробку фону й масштаб узгодженої фільтрації для оцінювання якості виявлення, координатної точності та швидкодії конвеєра. Стенд містить камеру MER3-138-136G3M-P-SWIR F02 (Китай) із сенсором Sony IMX990 (Японія): роздільна здатність 1280 × 1024 пікселів, розмір пікселя 5 × 5 мкм, діапазон чутливості приблизно 0,4–1,65 мкм [24]. Об’єктив VA-LCM-1.3MP-12MM-F1.8-020-SWIR (Китай) має фокусну відстань 12 мм, відносний отвір до 1,8 та поле зору близько 30° по горизонталі й 24° по вертикалі [25]. Фон задавали на білому матовому екрані 4 з окремим освітлювачем 6, змінюючи розподіл освітленості або проєктуючи ландшафт. Темні або світлі кульки із зображеннями діаметром 2–5 пікселів переміщували електромеханічним приводом у площині 3 по близькій до прямолінійної траєкторії. Швидкість узгоджували з міжкадровим інтервалом для зміщення зображення щонайменше на два пікселі за кадр. Об’єктив фокусували на площині руху, де 1 мм відповідав двом пікселям сенсора, а поле зору становило приблизно 65 × 52 см.

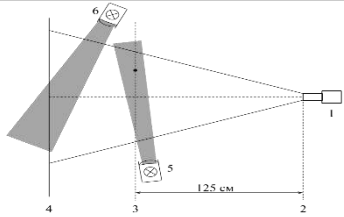


Рисунок 1. Принципова схема випробувального стенда: 1 – камера відеоспостереження; 2 – передня головна площина об'єктива камери; 3 – площина руху об'єкта; 4 – площина фону; 5 – освітлювач об'єкта; 6 – освітлювач фону

Експериментальні фактори охоплювали Етапи 0, 2 та 4 внутрішньокадрової обробки (ВКО). На Етапі 0 застосовували усереднювальне бінування з фактором $k \in \{1,2,4\}$: k = 1 – без бінування; k = 2 – бінування 2 × 2; k = 4 – бінування 4 × 4. На Етапі 2 порівнювали корекцію нерівномірності фону гаусовим згладжуванням і діленням (Gaussian Division, GD), міжкадровий інверсний медіанний фільтр (МКМФ), внутрішньокадровий просторовий інверсний медіанний фільтр (Median), послідовності GD→МКМФ, МКМФ→GD, Median→МКМФ, МКМФ→Median та контрольний варіант без Етапу 2. На Етапі 4 варіювали K – очікуваний лінійний розмір зображення об'єкта в пікселях, що задає масштаб ядра узгодженого фільтра. Досліджені значення наведено разом із результатами. Для порівняння відібрано натурні датасети D1–D3 з визначеними умовами знімання. Модельні датасети охоплювали: D4 – об'єкти та шум без структурованих завад; D5 – синусоїдальну просторову неоднорідність фону; D6 – плавну великомасштабну градієнтну неоднорідність; D7 – фіксовану просторову неоднорідність матриці (FPN) та гарячі пікселі; D8 – нерухоме локальне засвічення; D9 – засвічення з міжкадровим зміщенням; D10 – засвічення зі змінною в часі інтенсивністю; D11 – інтенсивну засвітку з насиченням частини зображення; D12 – поєднання синусоїдальної й градієнтної неоднорідностей, FPN і декількох типів засвічення. Сукупно досліджено близько 1000 конфігурацій для 12 датасетів. Парето-аналіз виконували окремо для кожного датасету. Відкидали конфігурації з NFD/Fr > 0,5, після чого залишали рішення з PD у межах 3 % від максимального значення; якщо їх було менше трьох, допуск розширювали до 8 %. Серед відібраних рішень визначали недоміновані за критеріями СКВху → min та ВКО FPS → max: для них не існує іншої конфігурації, не гіршої за обома критеріями та кращої хоча б за одним. Для практичної Парето-множини рішення з відмінністю СКВху не більше ніж на 10 % вважали рівноцінними за точністю й надавали перевагу конфігурації з більшим FPS.

Багатостадійний конвеєр обробки зображень короткохвильового інфрачервоного діапазону

Конвеєр обробляє серію SWIR-кадрів і формує вимірювання параметрів об'єктів для подальшої міжкадрової обробки. Етапи 0–8 поєднують просторові операції з часовим оцінюванням фону; послідовність етапів і передавання даних наведено на рис. 2.

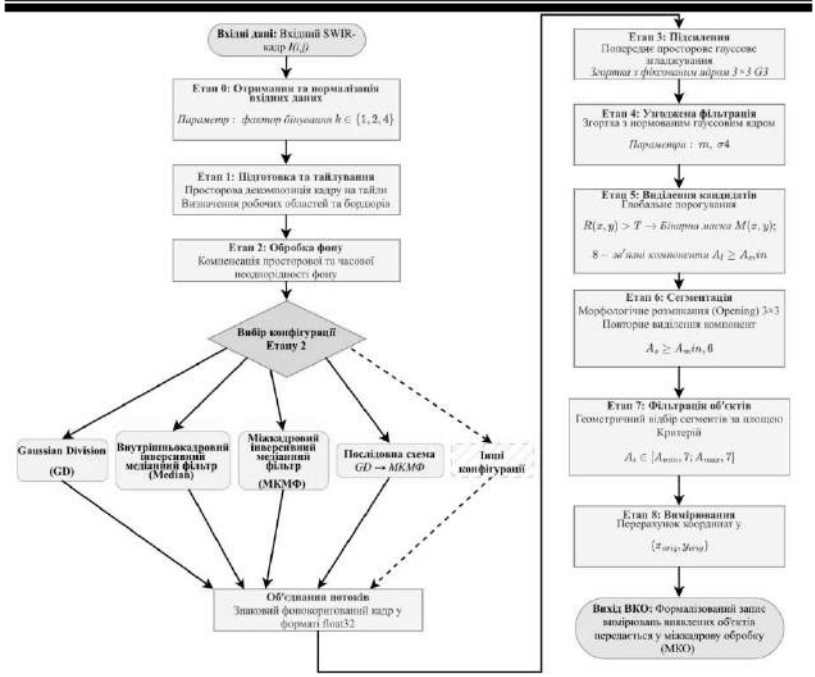


Рисунок 2. Блок-схема багатостадійного конвеєра внутрішньокадрової обробки SWIR-зображень

Штриховим контуром на схемі позначено додаткові комбіновані конфігурації для адаптації конвеєра до специфічних умов зйомки різних датасетів. На Етапі 0 застосовують усереднювальне бінування з фактором $k \in N, k \geq 1$. Для кадру шириною W і висотою H використовують лише повні блоки k × k; розміри робочої області становлять:

$$W_k = k\left\lfloor \frac{W}{k} \right\rfloor, \quad H_k = k\lfloor H / k \rfloor. \tag{1}$$

$$W_b = \frac{W_k}{k}, \quad H_b = \frac{H_k}{k}. \tag{2}$$

Яскравість бінованого пікселя з індексами (p, q) обчислюють усередненням блока k × k з округленням до найближчого цілого:

$$B(p,q) = round\left(\frac{1}{k^2} \sum_{s=0}^{k-1} \sum_{r=0}^{k-1} I(pk + r, qk + s) \right), \tag{3}$$

де $I(i, j)$ – значення яскравості пікселя вихідного зображення, а $B(p,q)$ – значення відповідного пікселя після бінування.

Координати центра блока, що відповідає бінованому пікселю (p,q), у вихідному кадрі дорівнюють:

$$x^{(0)}_{\{pq\}} = pk + \frac{k}{2}, \quad y^{(0)}_{\{pq\}} = qk + \frac{k}{2}. \tag{4}$$

Якщо координати бінованого кадру задають центрами пікселів, тобто $x^{(b)} = p + 1/2$ та $y^{(b)} = q + 1/2$, перерахунок має вигляд:

$$x^{(0)} = k\, x^{(b)}, \quad y^{(0)} = k\, y^{(b)}, \tag{5}$$

де $x^{(o)}$, $y^{(0)}$ – координати у вихідному кадрі.

Відкидання неповних правих і нижніх блоків не змінює початку робочої області, тому додаткового координатного зсуву не вводять.

На Етапі 1 кадр поділяють на тайли з бордюрами із сусідніх пікселів для локальних операцій біля меж. Обчислення використовують розширену область, а результати формуються лише для внутрішньої робочої області тайла. На Етапі 2 МКМФ обчислює часову медіану просторово відповідних пікселів каузальної послідовності кадрів. Нехай t – номер поточного кадру, K – кількість відібраних кадрів, $s \geq 1$ – крок відбору. Кадр включають до історії за умовою:

$$t \bmod s = 0, s \geq 1. \tag{6}$$

Після накопичення K кадрів попіксельна часова медіана для q-го відібраного кадру визначається як:

$$M_{tq}(x, y) = median\left\{ I_{(q-j)s}(x, y) : j = 0, \ldots, K-1 \right\}. \tag{7}$$

У реалізації $K \in \{3,5\}$. Після накопичення K кадрів медіану оновлюють на відібраних кадрах, а на проміжних використовують останню обчислену оцінку. Номер останнього відібраного кадру визначається як:

$$\tau(t) = s\lfloor t / s \rfloor. \tag{8}$$

$$M_t(x, y) = M_{\tau(t)}(x, y), \quad t \geq (K-1)s. \tag{9}$$

Після початкового накопичення фонокоригований залишок кожного вхідного кадру визначається відніманням медіанної оцінки:

$$R_t(x, y) = I_t(x, y) - M_t(x, y), \ t \geq (K-1)s. \tag{10}$$

Залишок зберігається у знаковому форматі float32. Якщо МКМФ завершує Етап 2, результат передається далі без обмеження діапазону, масштабування та додатного зміщення. Параметри K і s задають часовий розмах вікна:

$$\Delta t_{window} = (K-1)s. \tag{11}$$

ВКМФ компенсує крупноструктурні просторові неоднорідності фону. Передбачено два конфігураційні варіанти: просторовий інверсний медіанний фільтр і ділення на гауссово згладжене зображення.

Для внутрішньокадрового інверсного медіанного фільтра нехай $X_t(x, y)$ – поточне зображення, а L × L – квадратне вікно непарного розміру. Його радіус r та множина значень локального околу задаються співвідношеннями:

$$L = 2r + 1; \tag{12}$$

$$W_{x,y} = \left\{ X_t(x+u, y+v) : -r \leq u \leq r, -r \leq v \leq r \right\}. \tag{13}$$

Локальну медіанну оцінку крупноструктурного фону віднімають від поточного зображення:

$$M_t(x,y) = median\left(W_{x,y}\right); \tag{14}$$

$$R_t(x,y) = X_t(x,y) - M_t(x,y). \tag{15}$$

Результат зберігається у знаковому float32-поданні. Розмір вікна L пов'язується з характерним очікуваним просторовим розміром зображення об'єкта d_{obj} через емпіричний масштабний коефіцієнт C_L:

$$L \approx c_L d_{obj}. \tag{16}$$

Для GD фон оцінюють гауссовим згладжуванням. За коефіцієнта зменшення роздільності $d > 1$ використовують зменшену копію з подальшим поверненням карти фону до робочої роздільності:

$$B_G = Upsample\left[G_{\sigma d} * Downsample(I,d)\right], \tag{17}$$

де G – нормоване двовимірне гауссівське ядро, σ – його масштаб у пікселях початкового зображення, $B_G(x, y)$ – карта оціненого фону.

Середній рівень цієї карти C визначається по всій робочій області:

$$C = \frac{\sum_{y=0}^{H-1}\sum_{x=0}^{W-1} B_G(x,y)}{WH}. \tag{18}$$

Для захисту від малого знаменника та обмеження локального підсилення формується величина $D(x,y)$, де $\varepsilon > 0$ є захисним додатком, а $g_{max} \geq 1$ – верхньою межею локального коефіцієнта підсилення:

$$D(x,y) = max\left(B_G(x,y) + \varepsilon, \frac{C}{g_{max}}\right). \tag{19}$$

Знаковий фонокоригований результат GD визначається виразом:

$$R_G(x,y) = \left[I(x,y) - B_G(x,y)\right]\frac{C}{D(x,y)}. \tag{20}$$

Множник $C/D(x,y)$ масштабує різницю між зображенням і фоном без зміни її знака. Результат зберігається у форматі float32.

На Етапі 3 фонокориговане зображення $I_C(\underline{x,y})$ згладжують фіксованим гауссовим ядром 3 × 3. Параметр σ_3 визначає його ваги; результат $R_3(x,y)$ обчислюється згорткою:

$$R_3(x,y) = \sum_{i=-1}^{1}\sum_{j=-1}^{1} G_3(i,j)\, I_c(x-i, y-j), \tag{21}$$

де $G_3(i, j)$ – нормовані коефіцієнти гауссового ядра 3 × 3.

На Етапі 4 зображення Етапу 3 фільтрують ядром, що моделює очікуваний просторовий профіль об'єкта, формуючи неперервну карту відгуку $R(x,y)$.

Очікуваний просторовий профіль апроксимується двовимірною ізотропною гауссовою функцією. Для координат u і v відносно центра зображення об'єкта та параметра ширини профілю σ_4 модель має вигляд:

$$g(u,v) = exp\left[-\frac{u^2+v^2}{2\sigma_4^{\,2}}\right]. \tag{22}$$

Ширина профілю σ_4 і непарний розмір ядра m задаються окремо:

$$m = 2r + 1, \tag{23}$$

де r – радіус ядра.

Дискретна область його координат визначається як:

$$u, v \in \{-r, -r+1, \ldots, 0, \ldots, r-1, r\}. \tag{24}$$

За заданих m і σ_4 ненормовані коефіцієнти ядра дорівнюють значенням гауссової моделі:

$$\tilde{H}(u,v) = exp\left[-\frac{u^2+v^2}{2\sigma_4^2}\right], \; u, v = -r, \ldots, r. \tag{25}$$

Сума ненормованих коефіцієнтів дорівнює:

$$C = \sum_{u=-r}^{r}\sum_{v=-r}^{r}\tilde{H}(u,v). \tag{26}$$

А нормоване ядро визначається співвідношенням:

$$H(u,v) = \frac{\tilde{H}(u,v)}{C}. \tag{27}$$

Нормування зберігає гауссову форму ядра й забезпечує одиничну суму коефіцієнтів. Центральна симетрія робить кореляційний і згортковий записи еквівалентними. Для вхідного зображення $E(x,y)$:

$$R(x,y) = \sum_{u=-r}^{r}\sum_{v=-r}^{r}H(u,v)E(x+u, y+v). \tag{28}$$

За незмінних m і σ_4 ядро $H(u,v)$ формують один раз для серії, а карту $R(x,y)$ обчислюють для кожного тайла.

На Етапі 5 глобальний поріг T перетворює карту відгуку $R(x,y)$ на бінарну маску:

$$M(x,y) = \begin{cases} 255, & R(x,y) > T, \\ 0, & R(x,y) \le T. \end{cases} \tag{29}$$

У бінарній масці формують 8-зв'язні компоненти та відбирають їх за площею A_l з мінімально допустимим значенням A_{min}:

$$A_l \ge A_{min}. \tag{30}$$

Прийняті компоненти утворюють множину первинних кандидатів.

На Етапі 6 бінарну маску уточнюють без повторного порогування. У реалізованій конфігурації застосовують морфологічне розмикання множини пікселів переднього плану F прямокутним структурним елементом B розміру 3 × 3:

$$F \circ B = (F \ominus B) \oplus B. \tag{31}$$

Після морфологічної зміни областей 8-зв'язні компоненти формують повторно. До нових компонент із площею A_s застосовують окремий критерій мінімальної площі Етапу 6:

$$A_s \ge A_{min}, 6. \tag{32}$$

Прийняті компоненти перетворюються на сегменти гіпотетичних об'єктів для подальшого геометричного відбору. На Етапі 7 сегменти фільтрують виключно за площею. Для піксельної області Ω_i і-го сегмента площа дорівнює:

$$A_i = |\Omega_i|. \tag{33}$$

Сегмент приймається, якщо його площа задовольняє умову:

$$A_i \geq A_{\min,7} \wedge \left(A_{\max,7} = 0 \vee A_i \leq A_{\max,7}\right), \tag{34}$$

де $A_{min,7}$ і $A_{max,7}$ – нижня та верхня межі площі відповідно; $A_{max,7} = 0$ означає відсутність верхньої межі.

На Етапі 8 для відібраних сегментів обчислюють сигнально-фонові характеристики, виконують фінальну внутрішньокадрову перевірку й формують вимірювання. Інтенсивності визначають за фонокоригованим зображенням $I_c(x,y)$ з Етапу 2. Для оцінювання локального фону використовується реальна піксельна область сегмента Ω_s. Нехай B_r – прямокутний структурний елемент розміру $(2r+1)\times(2r+1)$, де r задає ширину локального фонового околу, а F – множина пікселів переднього плану поточної маски. Спочатку область сегмента дилатується:

$$D_s = \Omega_s \oplus B_r. \tag{35}$$

Після цього з дилатованої області вилучаються всі пікселі переднього плану, і локальна фонова область визначається як:

$$B_s = D_s \cap F^c. \tag{36}$$

Отже, $B_s \cap \Omega_s = \varnothing$. Обмежувальний прямокутник задає лише технічну область обчислень. Середнє значення сигналу в локальній фоновій області дорівнює:

$$I_{bg,s} = \frac{1}{|B_s|} \sum_{(x,y)\in B_s} I_c(x,y). \tag{37}$$

Стандартне відхилення локального фонового сигналу становить:

$$\sigma_{bg,s} = \sqrt{\frac{1}{|B_s|} \sum_{(x,y)\in B_s} \left(I_c(x,y) - I_{bg,s}\right)^2}. \tag{38}$$

Середню інтенсивність сегмента визначають за його реальною піксельною областю:

$$I_s = \frac{1}{A_s} \sum_{(x,y)\in\Omega_s} I_c(x,y),\ A_s = |\Omega_s|. \tag{39}$$

Додатковою характеристикою сегмента може бути максимальна інтенсивність:

$$I_{\max,s} = \max_{(x,y)\in\Omega_s} I_c(x,y). \tag{40}$$

Інтегральний надлишковий сигнал характеризує сумарне перевищення над локальним фоном:

$$S_{exc,s} = \sum_{(x,y)\in\Omega_s} \left[I_c(x,y) - I_{bg,s}\right] = A_s\left(I_s - I_{bg,s}\right). \tag{41}$$

Для фінальної внутрішньокадрової перевірки формується безрозмірна SNR-подібна статистика:

$$q_s = \frac{I_s - I_{bg,s}}{\sigma_{bg,s}}. \tag{42}$$

Гіпотеза про наявність зображення об'єкта в межах ВКО приймається за критерієм:

$$q_s \geq q_{cr}, \tag{43}$$

де порогове значення q_{cr} є окремим порогом Етапу 8. Запис прийнятого вимірювання містить ідентифікатор кадру, оцінку положення, обмежувальний прямокутник, площу, сигнальні й фонові характеристики та q_s. Для локальної оцінки положення $(\hat{x}_s, \hat{y}_s)$ та зміщення j-го тайла $(x_{0,j}, y_{0,j})$ перехід до координат повного поточного кадру визначається як:

$$\hat{x}_{s,fr} = \hat{x}_s + x_{0,j},\ \hat{y}_{s,fr} = \hat{y}_s + y_{0,j}. \tag{44}$$

Після врахування зміщення тайла координати бінованого кадру з фактором k перераховують до системи вихідного небінованого кадру:

$$x_{orig} = kx_{bin},\ y_{orig} = ky_{bin}. \tag{45}$$

Внутрішньокадрове виявлення ще не підтверджує наявності реального рухомого об'єкта. Вимірювання передаються до міжкадрової обробки (МКО), основною складовою якої є трекінг.

Результати

Закономірності оцінювали за повним масивом експериментальних даних. У табл. 1–3 наведено вибрані результати D1, у табл. 4 – D3, D11 і D12.

Таблиця 1

Показники точності оцінювання координат положення об'єкта

№	Конфігурація	$\overline{\Delta x}$, px	$\overline{\lvert\Delta x\rvert}$, px	$\overline{\Delta y}$, px	$\overline{\lvert\Delta y\rvert}$, px	σ_x, px	σ_y, px	σ_{xy}, px
	№датасету = 1; $\overline{\mathrm{SNR}} = 645.09 - 673.39$, $N_{exp1} = 86$							
1	GD→МКМФ, ББ, К10	0.06	0.91	-0.04	0.74	1.0960	0.8910	1.4100
2	GD→МКМФ, ББ, К3	0.05	0.91	-0.05	0.74	1.0970	0.8870	1.4100
3	МКМФ→GD, ББ, К10	0.05	0.91	-0.03	0.74	1.0960	0.8870	1.4100
4	МКМФ→GD, ББ, К3	0.05	0.91	-0.05	0.74	1.0970	0.8870	1.4100
5	Median, ББ, К10	0.22	0.92	-0.17	0.76	1.1000	0.8840	1.4100
6	GD, ББ, К10	0.19	0.92	-0.13	0.75	1.1070	0.8900	1.4200
7	МКМФ, ББ, К10	0.04	0.92	-0.03	0.74	1.1000	0.8910	1.4200
8	МКМФ, ББ, К3	0.04	0.91	-0.04	0.74	1.0980	0.8890	1.4100
9	GD→МКМФ, 2×2, К5	0.01	0.95	-0.01	0.78	1.1490	0.9460	1.4900
10	GD→МКМФ, 2×2, К3	0.01	0.96	-0.01	0.79	1.1590	0.9600	1.5100
11	GD→МКМФ, 2×2, К10	-0.12	0.96	0.10	0.80	1.1610	0.9770	1.5200
12	МКМФ→GD, 2×2, К5	0.01	0.95	0.00	0.77	1.1440	0.9390	1.4800
13	МКМФ→GD, 2×2, К3	0.02	0.95	-0.01	0.78	1.1500	0.9460	1.4900
14	Median→МКМФ, 2×2, К5	0.05	0.94	-0.03	0.77	1.1380	0.9350	1.4700
15	Median→МКМФ, 2×2, К3	0.05	0.95	-0.04	0.79	1.1560	0.9490	1.5000
16	МКМФ, 2×2, К5	0.00	0.95	0.01	0.77	1.1390	0.9420	1.4800
17	МКМФ, 2×2, К3	0.00	0.94	0.00	0.79	1.1400	0.9520	1.4900

№	Конфігурація	$\overline{\Delta x}$, px	$\overline{\lvert\Delta x\rvert}$, px	$\overline{\Delta y}$, px	$\overline{\lvert\Delta y\rvert}$, px	σ_x, px	σ_y, px	σ_{xy}, px
18	GD→МКМФ, 4×4, К3	-0.59	1.19	0.50	1.04	1.3320	1.2040	1.8000
19	МКМФ→GD, 4×4, К3	-0.62	1.22	0.50	1.02	1.3550	1.1920	1.8000
20	Median→МКМФ, 4×4, К3	-0.61	1.23	0.43	1.02	1.3740	1.1940	1.8200

Таблиця 2

Показники якості виявлення об'єктів спостереження

№	Конфігурація	PD	PFA	$\overline{N_{FD/Fr}}$
	№датасету = 1; $\overline{\text{SNR}} = 645.09 - 673.39$, $N_{exp1} = 86$			
1	GD→МКМФ, ББ, К10	1.00	8e-08	0.0044
2	GD→МКМФ, ББ, К3	1.00	8e-08	0.0044
3	МКМФ→GD, ББ, К10	1.00	6e-08	0.0033
4	МКМФ→GD, ББ, К3	1.00	8e-08	0.0044
5	Median, ББ, К10	1.00	2.68e-06	7.0256
6	GD, ББ, К10	0.99	2.81e-06	5.8500
7	МКМФ, ББ, К10	1.00	6e-08	0.0033
8	МКМФ, ББ, К3	1.00	8e-08	0.0044
9	GD→МКМФ, 2×2, К5	1.00	4e-08	0.0022
10	GD→МКМФ, 2×2, К3	1.00	4e-08	0.0022
11	GD→МКМФ, 2×2, К10	0.92	2e-08	0.0011
12	МКМФ→GD, 2×2, К5	1.00	2e-08	0.0011
13	МКМФ→GD, 2×2, К3	1.00	2e-08	0.0011
14	Median→МКМФ, 2×2, К5	1.00	2e-08	0.0011
15	Median→МКМФ, 2×2, К3	1.00	2e-08	0.0011
16	МКМФ, 2×2, К5	1.00	2e-08	0.0011
17	МКМФ, 2×2, К3	1.00	4e-08	0.0022
18	GD→МКМФ, 4×4, К3	0.99	4e-08	0.0022
19	МКМФ→GD, 4×4, К3	0.98	2e-08	0.0011
20	Median→МКМФ, 4×4, К3	0.98	2e-08	0.0011

Таблиця 3

Часові характеристики обробки

№	Конфігурація	Кадрів	Час, с	FPS	Читання, с	ВКО, с	ВКО FPS
	№датасету = 1; $\overline{\text{SNR}} = 645.09 - 673.39$, $N_{exp1} = 86$						
1	GD→МКМФ, ББ, К10	910	20.48	44.43	10.29	6.94	131.13
2	GD→МКМФ, ББ, К3	910	60.10	15.14	39.79	12.58	72.33
3	МКМФ→GD, ББ, К10	910	26.67	34.13	10.85	10.44	87.16
4	МКМФ→GD, ББ, К3	910	60.10	15.14	35.87	16.80	54.16
5	Median, ББ, К10	910	61.85	14.71	27.67	25.84	35.21
6	GD, ББ, К10	910	41.63	21.86	13.43	6.44	141.20
7	МКМФ, ББ, К10	910	61.83	14.72	46.13	8.26	110.22
8	МКМФ, ББ, К3	910	43.72	20.82	11.52	7.88	115.55
9	GD→МКМФ, 2×2, К5	910	37.88	24.02	16.58	2.13	427.90
10	GD→МКМФ, 2×2, К3	910	32.56	27.95	9.41	2.09	435.92

№	Конфігурація	Кадрів	Час, с	FPS	Читання, с	ВКО, с	ВКО FPS
11	GD→МКМФ, 2×2, K10	910	34.08	26.70	9.51	2.15	422.83
12	МКМФ→GD, 2×2, K5	910	32.59	27.92	10.64	2.77	328.95
13	МКМФ→GD, 2×2, K3	910	30.27	30.07	10.02	2.54	357.91
14	Median→МКМФ, 2×2, K5	910	33.28	27.34	14.32	7.40	122.97
15	Median→МКМФ, 2×2, K3	910	32.16	28.30	10.62	7.29	124.86
16	МКМФ, 2×2, K5	910	61.83	14.72	53.42	1.96	464.25
17	МКМФ, 2×2, K3	910	25.07	36.30	8.99	1.89	480.54
18	GD→МКМФ, 4×4, K3	910	17.81	51.09	10.41	0.82	1114.83
19	МКМФ→GD, 4×4, K3	910	21.71	41.92	10.12	0.83	1095.29
20	Median→МКМФ, 4×4, K3	910	31.25	29.12	12.91	2.11	431.97

Таблиця 4

Узагальнені показники для датасетів D3, D11 та D12

№	Конфігурація	σ_{xy}, px	PD	$\overline{N_{FD/Fr}}$	ВКО FPS
	№датасету = 3; $\overline{\mathrm{SNR}} = 499.84 - 535.91$, $N_{exp3} = 86$				
1	GD→МКМФ, ББ, K10	1.1100	0.99	0.0035	124.04
2	GD→МКМФ, ББ, K3	1.1200	1.00	0.1132	87.94
3	МКМФ→GD, ББ, K10	1.1300	1.00	0.0035	83.10
4	МКМФ→GD, ББ, K3	1.1100	1.00	0.1225	72.30
5	МКМФ, ББ, K3	1.1200	1.00	0.0922	114.26
6	МКМФ, ББ, K10	1.1200	0.99	0.0035	109.09
7	Median, ББ, K10	1.1500	1.00	7.0665	33.90
8	GD, ББ, K10	1.1400	1.00	1.0653	135.37
9	МКМФ→Median, ББ, K10	1.1200	0.99	0.0023	3.96
	№датасету = 11; $\overline{\mathrm{SNR}} = 8,2 - 19,7$, $N_{exp11} = 24$				
21	GD→МКМФ, ББ	1.4400	0.82	0.1200	42.46
22	МКМФ→GD, ББ	1.5600	0.93	1.2200	40.44
23	МКМФ, ББ	1.6500	0.94	0.2200	83.24
24	GD, ББ	1.2200	0.93	0.4000	54.99
25	Без S2, ББ	1.2900	0.76	1.1800	76.67
26	МКМФ→Median, ББ	2.2300	0.83	0.2800	2.67
31	Без S2, 2×2	1.3900	0.74	0.5600	370.64
37	Без S2, 4×4	1.6000	0.51	0.0400	1170.96
	№датасету = 12; $\overline{\mathrm{SNR}} = 180,2 - 280,3$, $N_{exp12} = 24$				
41	GD→МКМФ, ББ	0.6600	0.87	1.3800	32.77
42	МКМФ→GD, ББ	0.6500	0.88	0.2600	39.01
43	МКМФ, ББ	0.6700	0.81	0.3800	79.56
44	GD, ББ	0.6900	0.91	6.7600	57.70
45	Без S2, ББ	0.7300	0.52	0.0200	70.63
50	Без S2, 2×2	0.8300	0.52	0.0000	231.21
51	МКМФ→Median, ББ	0.8500	0.84	2.0800	2.66
57	Без S2, 4×4	1.1900	0.48	0.0200	812.35

Високе PD не гарантує малої кількості хибних виявлень. Для D1 без бінування при K10 методи Median, GD і МКМФ забезпечують PD = 0,99–1,00, але NFD/Fr становить відповідно 7,0256, 5,8500 і 0,0033 (табл. 2). Подібна відмінність спостерігається для D3 (табл. 4). Відносна ефективність методів Етапу 2 залежить від фонових умов.

За повним масивом даних порядок Median→МКМФ на D3 при бінуванні 2 × 2 і K5 забезпечує вищу швидкодію, ніж МКМФ→Median, за близької якості. На D11 при 4 × 4 швидший порядок Median→МКМФ супроводжується нижчим PD. Виграш у швидкодії може супроводжуватися зниженням якості виявлення. Вимкнення Етапу 2 часто зменшує обчислювальні витрати, але не гарантує найбільшої швидкодії.

Для D11 при 4 × 4 воно забезпечує 1170,96 ВКО FPS за PD = 0,51, а для D12 у трьох режимах бінування PD становить 0,48–0,52 (табл. 4). Бінування також створює компроміс: для GD→МКМФ на D1 при K3 перехід від обробки без бінування до 4 × 4 підвищує ВКО FPS із 72,33 до 1114,83, але збільшує СКВху з 1,41 до 1,80 рх і знижує PD з 1,00 до 0,99 (табл. 1–3). Для дослідження K Етапу 4 спосіб обробки фону фіксували як МКМФ. Варіювали K і бінування (без бінування, 2 × 2, 4 × 4) для D1 із зображенням об'єкта приблизно 8–10 рх та D4 із розміром 36 × 36 рх.

Таблиця 5

D1 (натурний): СКВху залежно від розміру ядра узгодженого фільтру *K*, рх

Конфігурація	3	5	7	9	10	13	16	19	24	37	45	55	70
МКМФ, ББ	1.41	3.47	3.44	3.44	1.42	3.43	2.94	2.96	2.63	2.14	3.04	–	–
МКМФ, 2×2	1.49	1.48	3.35	3.20	1.55	2.34	3.07	2.99	0.00	–	–	–	–
МКМФ, 4×4	1.79	0.00	5.25	2.22	1.95	–	–	–	–	–	–	–	–

Таблиця 6

D1 (натурний): PD залежно від розміру ядра узгодженого фільтру *K*, рх

Конфігурація	3	5	7	9	10	13	16	19	24	37	45	55	70
МКМФ, ББ	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.95	0.44	–	–
МКМФ, 2×2	1.00	1.00	1.00	1.00	0.64	1.00	0.79	0.53	0.01	–	–	–	–
МКМФ, 4×4	0.93	0.02	0.01	0.01	0.63	–	–	–	–	–	–	–	–

На D1 залежності СКВху(K) і PD(K) немонотонні (табл. 5, 6). Без бінування PD = 1,00 зберігається при *K* = 3–24, а при *K* = 45 знижується до 0,44. За бінування погіршення виявлення проявляється при менших K. Причини локальних покращень СКВху поблизу *K* = 3 та *K* = 10 не встановлено. Для модельного датасету D4 найкраща координатна точність без бінування спостерігається при *K* = 24, у режимі 2 × 2 – при *K* = 9, а за 4 × 4 зміщується в область малих *K* (табл. 7).

Таблиця 7

D4 (модельний): СКВху залежно від розміру ядра узгодженого фільтру *K*, рх

Конфігурація	3	5	7	9	10	13	16	19	24	37	45	55	70
МКМФ,ББ	2.47	2.30	2.13	1.88	1.95	1.89	1.66	1.61	1.42	1.63	1.88	1.94	2.44
МКМФ, 2×2	1.79	1.69	1.51	1.46	1.75	1.71	1.66	1.68	1.97	2.40	2.58	3.21	3.43
МКМФ, 4×4	1.91	1.90	2.12	2.08	2.08	2.58	2.58	2.57	2.84	3.51	3.64	–	–

Таблиця 8

D4 (модельний): PD залежно від розміру ядра узгодженого фільтру *K*, px

Конфігурація	3	5	7	9	10	13	16	19	24	37	45	55	70
МКМФ, ББ	0.49	0.48	0.43	0.37	0.94	0.93	0.87	0.85	0.73	0.95	0.96	0.91	0.90
МКМФ, 2×2	0.83	0.82	0.78	0.72	0.96	0.96	0.93	0.91	0.91	0.81	0.59	0.47	0.15
МКМФ, 4×4	0.90	0.89	0.93	0.90	0.81	0.92	0.78	0.67	0.34	0.10	0.03	–	–

Ймовірність виявлення PD для D4 також чутлива до масштабу: за бінування 2 × 2 значення PD = 0,96 при $K = 10$ і 13 знижується до 0,15 при $K = 70$, а за 4 × 4 спад відбувається раніше: PD = 0,34 при $K = 24$ і 0,03 при $K = 45$ (табл. 8). Раціональна область K залежить від масштабу зображення об'єкта після бінування; універсального оптимуму для різних класів фону не встановлено.

Обговорення результатів

За процедурою для кожного датасету сформовано формальну Парето-оптимальну множину (ПОМФ) і практичну множину (ПОМУН), що враховує нечутливість до малих змін $\text{СКВ}_{xy} \pm 10\%$. У табл. 9 наведено елементи ПОМУН.

Таблиця 9

Практично раціональні конфігурації конвеєра (ПОМУН)

№	Конфігурація	σ_{xy}, px	PD	$\overline{N_{FD/Fr}}$	ВКО FPS	ПОМУН
	№датасету = 1; $\overline{\text{SNR}} = 645.09 - 673.39$, $N_{exp1} = 86$					
17	МКМФ, 2×2, КЗ	1.4900	1.00	0.0022	480.54	✓
18	GD→МКМФ, 4×4, КЗ	1.8000	0.99	0.0022	1114.83	✓
	№датасету = 2; $\overline{\text{SNR}} = 407.71 - 524.87$, $N_{exp2} = 86$					
33	МКМФ→GD, 2×2, КЗ	1.4200	1.00	0.0451	356.13	✓
	№датасету = 3; $\overline{\text{SNR}} = 499.84 - 535.91$, $N_{exp3} = 86$					
55	МКМФ, 2×2, КЗ	1.2000	1.00	0.0117	466.42	✓
	№датасету = 4; $\overline{\text{SNR}} = 7,8 - 17,2$, $N_{exp4} = 24$					
65	Без S2, ББ	1.3300	0.98	0.0400	101.20	✓
70	GD, 2×2	1.5000	0.99	0.1400	283.21	✓
76	GD, 4×4	1.9100	0.98	0.2400	904.98	✓
	№датасету = 5; $\overline{\text{SNR}} = 7,7 - 17,9$, $N_{exp5} = 24$					
89	МКМФ, 2×2	1.7500	0.89	0.1000	352.98	✓
95	МКМФ, 4×4	2.0700	0.87	0.2600	974.66	✓
	№датасету = 6; $\overline{\text{SNR}} = 7,7 - 18,5$, $N_{exp6} = 24$					
104	GD, ББ	1.2100	0.99	0.3000	53.19	✓
	№датасету = 7; $\overline{\text{SNR}} = 8,1 - 20,0$, $N_{exp7} = 24$					
131	Без S2, 2×2	1.5800	0.98	0.3200	386.25	✓
136	GD, 4×4	1.9500	0.94	0.2400	974.66	✓

№	Конфігурація	σ_{xy}, px	PD	$\overline{N_{FD/Fr}}$	ВКО FPS	ПОМУН
	№датасету = 8; $\overline{\text{SNR}} = 7,8 - 18,8$, $N_{exp8} = 24$					
149	МКМФ, 2×2	1.6700	0.91	0.0600	366.57	✓
155	МКМФ, 4×4	2.0600	0.89	0.0200	892.86	✓
	№датасету = 9; $\overline{\text{SNR}} = 14,0 - 20,4$, $N_{exp9} = 24$					
164	GD, ББ	0.8100	0.98	0.0400	58.40	✓
167	GD→МКМФ, 2×2	1.2200	0.97	0.2000	236.41	✓
173	GD→МКМФ, 4×4	1.6300	0.96	0.2400	725.69	✓
	№датасету = 10; $\overline{\text{SNR}} = 75,8 - 240,3$, $N_{exp10} = 24$					
182	МКМФ→GD, ББ	0.3400	0.96	0.2200	37.66	✓
187	GD→МКМФ, 2×2	0.4500	0.97	0.2400	212.18	✓
194	МКМФ→GD, 4×4	0.7600	0.94	0.2600	675.22	✓
	№датасету = 11; $\overline{\text{SNR}} = 8,2 - 19,7$, $N_{exp11} = 24$					
204	GD, ББ	1.2200	0.93	0.4000	54.99	✓
209	МКМФ, 2×2	1.6600	0.90	0.0400	361.27	✓
215	МКМФ, 4×4	2.0300	0.90	0.1400	877.19	✓
	№датасету = 12; $\overline{\text{SNR}} = 180,2 - 280,3$, $N_{exp12} = 24$					
226	GD→МКМФ, 2×2	0.6700	0.87	0.4400	167.95	✓
229	GD, 2×2	0.7400	0.87	0.3200	376.51	✓

Сумарно для 12 датасетів отримано 40 конфігурацій ПОМФ і 25 ПОМУН. Відсіяно рішення, для яких малий виграш у точності не компенсує втрату швидкодії. Наприклад, на D1 GD→МКМФ без бінування з 1,41 px і 131,13 ВКО FPS поступається за практичним вибором МКМФ, 2 × 2, К3 з 1,49 px і 480,54 ВКО FPS. Багатокритеріальний підхід застосовують також до розподілу обмежених ресурсів сенсорних мереж [27].

У ПОМУН зберігаються всі режими бінування: 12 конфігурацій із 2 × 2, вісім із 4 × 4 і п'ять без бінування. Для D4 представлені всі три режими, що відображає компроміс між точністю та швидкодією за прийнятної якості виявлення. Універсального способу обробки фону не виявлено. Для D5 ПОМУН містить лише МКМФ із бінуванням 2 × 2 і 4 × 4, для D6 – GD без бінування, для D10 – послідовності GD→МКМФ і МКМФ→GD. Конкретний вибір залежить від датасету. Окремий Median і послідовності Median→МКМФ та МКМФ→Median не увійшли до жодної ПОМФ. Практичні альтернативи утворюють МКМФ, GD та їх послідовності; для двох датасетів зберігся варіант без Етапу 2. Конфігурацію з ПОМУН обирають відповідно до вимог точності й швидкодії конкретної системи.

Висновки

Розроблено багатостадійний конвеєр обробки послідовностей SWIR-зображень малорозмірних рухомих об'єктів, що охоплює Етапи 0–8 – від

отримання й нормалізації кадру до формування вимірювань. Конвеєр поєднує просторову обробку кадрів із часовим контекстом оцінювання фону та визначає узгоджену послідовність підготовки даних, компенсації фону, фільтрації, сегментації й оцінювання параметрів об'єктів. Експериментальне дослідження програмного бінування, способів і порядку обробки фону та масштабу ядра узгодженої фільтрації виявило компроміси між якістю виявлення, координатною точністю та швидкодією. Підвищення швидкодії внаслідок бінування може супроводжуватися втратою точності й погіршенням виявлення. Ефективність обробки фону залежить від характеру завад і порядку процедур. Вплив розміру ядра є немонотонним, а його раціональна область залежить від масштабу зображення об'єкта після бінування. Багатокритеріальний аналіз виконано окремо для кожного з 12 наборів даних. Після відбору за показниками виявлення конфігурації порівнювали за координатною похибкою та швидкодією. Урахування практичної нечутливості до малих відмінностей координатного показника (до 10 %) скоротило загальну кількість альтернатив із 40 конфігурацій формальної Парето-множини до 25 практично раціональних. Універсальної оптимальної конфігурації не встановлено; вибір залежить від умов спостереження та пріоритетів конкретної системи. Отримані закономірності стосуються досліджених натурних і модельних даних, режимів обробки та реалізації конвеєра. Для інших сенсорів, масштабів об'єктів і фонових умов склад раціональних конфігурацій потребує повторного оцінювання. Практичними обмеженнями є ручне налаштування глобального порогу та граничного SNR-показника, а також обчислювальні витрати послідовної просторово-часової обробки фону, які можуть ускладнювати застосування конвеєра на малопотужних системах.

Подальша робота передбачає автоматизацію вибору конфігурацій із практичної Парето-множини на основі класифікації фонової обстановки. Адаптацію до динамічних змін завад та освітленості планується реалізувати через інтеграцію компактних моделей машинного навчання, що потребує окремої експериментальної перевірки.

Література

[1] Vlasenko, V., Khlamov, S., & Savanevych, V. (2024). Devising a procedure for the brightness alignment of astronomical frames background by a high frequency filtration to improve accuracy of the brightness estimation of objects. Eastern-European Journal of Enterprise Technologies, 2(2 (128)), 31-38. https://doi.org/10.15587/1729-4061.2024.301327.

[2] Sorensen, C. M. (2022). Light Scattering and Absorption by Particles. IOP Publishing. https://doi.org/10.1088/978-0-7503-5157-7.

[3] Peroni, R., Penide, G., Cornet, C., Pujol, O., & Pierangelo, C. (2025). Water vapor content retrieval under cloudy sky conditions from SWIR satellite measurements in the context of C3IEL space mission project. Atmospheric Measurement Techniques, 18, 7369-7385. https://doi.org/10.5194/amt-18-7369-2025.

[4] Wiley, L., Cavanaugh, R., Follansbee, J., Burrell, D., Grimming, R., Pimpinella, R., Voss, J., Furxhi, O., & Driggers, R. (2023). Comparison of reflective band (Vis, NIR, SWIR, eSWIR) performance in daytime reduced illumination conditions. Applied Optics, 62(31), 8316-8326. https://doi.org/10.1364/AO.495832.

[5] Chen, Q., Liu, X., Du, L., Song, B., Sun, X., & Shen, Z. (2026). Three-band SWIR imaging for Pix2Pix-based colorization. Applied Optics, 65(11), 3798-3814. https://doi.org/10.1364/AO.590489.

[6] Leslie, P., Cavanaugh, R. C., Jordan, S., Wiley, L., Jacobs, E., Driggers, R., & Conroy, J. (2024). Visible, NIR, SWIR, and eSWIR urban and rural scene contrast comparison. Applied Optics, 63(7), 1839-1846. https://doi.org/10.1364/AO.510226.

[7] Khlamov, S., Savanevych, V., Tabakova, I., & Trunova, T. (2022). The astronomical object recognition and its near-zero motion detection in series of images by in situ modeling. In 2022 International Conference on Systems, Signals, and Image Processing (IWSSIP). (pp. 1-4). IEEE. https://doi.org/10.1109/IWSSIP55020.2022.9854475.

[8] Masias, M., Freixenet, J., Lladó, X., & Peracaula, M. (2012). A review of source detection approaches in astronomical images. Monthly Notices of the Royal Astronomical Society, 422(2), 1674-1689. https://doi.org/10.1111/j.1365-2966.2012.20742.x.

[9] Zhao, M., Li, W., Li, L., Hu, J., Ma, P., & Tao, R. (2022). Single-frame infrared small-target detection: A survey. IEEE Geoscience and Remote Sensing Magazine, 10(2), 87-119. https://doi.org/10.1109/MGRS.2022.3145502.

[10] Kou, R., Wang, C., Peng, Z., Zhao, Z., Chen, Y., Han, J., Huang, F., Yu, Y., & Fu, Q. (2023). Infrared small target segmentation networks: A survey. Pattern Recognition, 143, 109788. https://doi.org/10.1016/j.patcog.2023.109788.

[11] Yang, H., Mu, T., Dong, Z., Zhang, Z., Wang, B., Ke, W., Yang, Q., & He, Z. (2024). PBT: Progressive background-aware transformer for infrared small target detection. IEEE Transactions on Geoscience and Remote Sensing, 62, 1-13. https://doi.org/10.1109/TGRS.2024.3415080.

[12] Xu, M., Yu, C., Li, Z., Tang, H., Hu, Y., & Nie, L. (2025). HDNet: A hybrid domain network with multiscale high-frequency information enhancement for infrared small-target detection. IEEE Transactions on Geoscience and Remote Sensing, 63, 1-15. https://doi.org/10.1109/TGRS.2025.3574962.

[13] Zhang, J., Yang, H., & Sun, J. (2024). Infrared Small Target Detection Based on Transformer-Based Multi-scale Fusion Attention. Academic Journal of Computing & Information Science, 7(10), 97-104. https://doi.org/10.25236/AJCIS.2024.071014.

[14] Khlamov, S., Savanevych, V., Tabakova, I., Kartashov, V., Trunova, T., & Kolendovska, M. (2024). Machine Vision for Astronomical Images using The Modern Image Processing Algorithms Implemented in the CoLiTec Software. In Measurements and Instrumentation for Machine Vision. (pp. 269-310). CRC Press. https://doi.org/10.1201/9781003343783-12.

[15] Khlamov, S., Savanevych, V., Vlasenko, V., Briukhovetskyi, O., Trunova, T., Levykin, I., Shvedun, V., & Tabakova, I. (2023). Development of the matched filtration of a blurred digital image using its typical form. Eastern-European Journal of Enterprise Technologies, 1(9 (121)), 62-71. https://doi.org/10.15587/1729-4061.2023.273674.

[16] Lang, D., & Hogg, D. W. (2026). Principled point-source detection in collections of astronomical images. The Astronomical Journal, 171(4), 231. https://doi.org/10.3847/1538-3881/ae4505.

[17] Zheng, C., Pulido, J., Thorman, P., & Hamann, B. (2015). An improved method for object detection in astronomical images. Monthly Notices of the Royal Astronomical Society, 451(4), 4445-4459. https://doi.org/10.1093/mnras/stv1237.

[18] Xi, T., Yuan, L., & Sun, Q. (2022). A combined approach to infrared small-target detection with the alternating direction method of multipliers and an improved top-hat transformation. Sensors, 22(19), 7327. https://doi.org/10.3390/s22197327.

[19] Minaee, S., Boykov, Y. Y., Porikli, F., Plaza, A. J., Kehtarnavaz, N., & Terzopoulos, D. (2021). Image Segmentation Using Deep Learning: A Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 44(7), 3523-3542. https://doi.org/10.1109/TPAMI.2021.3059968.

[20] Khlamov, S., Savanevych, V., Briukhovetskyi, O., & Trunova, T. (2023). Big data analysis in astronomy by the Lemur software. In Proceedings of the IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo 2023). (pp. 5-8). IEEE. https://doi.org/10.1109/UkrMiCo61577.2023.10380398.
[21] Bellanger, M. (2024). Digital Signal Processing: Theory and Practice. Wiley.
[22] Burger, W., & Burge, M. (2022). Digital Image Processing: An Algorithmic Introduction. Springer Nature. https://doi.org/10.1007/978-3-031-05744-1.
[23] Khlamov, S., Savanevych, V., Briukhovetskyi, O., Tabakova, I., & Trunova, T. (2022). Astronomical knowledge discovery in databases by the CoLiTec software. In Proceedings of the 12th International Conference on Advanced Computer Information Technologies (ACIT 2022). (pp. 583-586). IEEE. https://doi.org/10.1109/ACIT54803.2022.9913188.
[24] DAHENG IMAGING. (2026). MER3-138-136G3M-P-SWIR F02. https://en.daheng-imaging.com/show-957-3243-1.html.
[25] VA Imaging. (2026). VA-LCM-1.3MP-12MM-F1.8-020-SWIR Lens SWIR. https://va-imaging.com/products/lens-swir-c-mount-1-3mp-12mm-f1-8-1-2-lcm-swir-1-3mp-12mm-f1-8-020.
[26] Li, Q., Zhang, W., Lu, W., & Wang, Q. (2025). Multibranch mutual-guiding learning for infrared small target detection. IEEE Transactions on Geoscience and Remote Sensing, 63, 1-10. https://doi.org/10.1109/TGRS.2025.3526754.
[27] Yu, Y., Tang, X., & Xie, G. (2026). Optimal Resource Allocation via Unified Closed-Form Solutions for SWIPT Multi-Hop DF Relay Networks. Sensors, 26(2), 512. https://doi.org/10.3390/s26020512.

MULTISTAGE SHORT-WAVE INFRARED IMAGE PROCESSING PIPELINE

Bondar Y.[1], Kutvytskyi M.[1],
Netrebin Y.[1], Dr. Sci., Savanevych V.[1], Ph.D., Khlamov S.[1],
Dr.Sci., Zelensky S.[2], Ph.D., Khoroshevska I.[3], Ph.D., Tabakova I.[1]
[1] Kharkiv National University of Radio Electronics, Ukraine,
[2] Taras Shevchenko National University of Kyiv, Ukraine,
[3] Simon Kuznets Kharkiv National University of Economics, Ukraine

Abstract. *Detecting small moving objects in short-wave infrared (SWIR) image sequences requires balancing detection quality, localization accuracy, and processing speed under spatially nonuniform and time-varying backgrounds. A multistage pipeline was developed from data preparation to measurement generation. Experiments on real and simulated data examined software binning, background-processing methods and their order, and matched-filter kernel scale. Faster processing through binning can reduce localization accuracy and detection quality. Background-processing effectiveness depends on observation conditions and procedure order, while suitable filter scale depends on object image size after binning. Pareto analysis was performed separately for each of 12 datasets. Accounting for practical insensitivity to small localization-error differences reduced the total number of nondominated configurations from 40 to 25 practical alternatives. No universally optimal configuration was identified. The results support pipeline parameter selection according to observation conditions and requirements for detection, accuracy, and processing speed.*

Keywords: *SWIR images, multistage processing, software binning, matched filtering, Pareto optimality, detection criterion, localization accuracy.*

UDC 519.23: 004.932.4
DOI

VOXEL-BASED MODELING OF THE EFFECT OF NON-UNIFORM FIBER DISTRIBUTION ON THE ELASTIC PROPERTIES OF FIBER-REINFORCED COMPOSITES

Ph.D., Vodka O.[1][0000-0002-4462-9869], Ph.D. Shapovalova M.[2][0000-0002-4771-7485], Ph.D. Misiura S.[3][0000-0002-5048-1610], Zhykhariev V.[4][0009-0006-0640-5895]

National Technical University "Kharkiv Polytechnic Institute", Ukraine
EMAIL:[1]oleksii.vodka@khpi.edu.ua, [2]Mariia.Shapovalova@khpi.edu.ua, [3]serhii.misiura@khpi.edu.ua, [4]Vladyslav.Zhykhariev@infiz.khpi.edu.ua

Abstract. *This paper investigates the influence of spatial non-uniformity of fiber distribution on the microstructural characteristics and effective elastic properties of unidirectional fiber-reinforced composites. A comprehensive methodology combining computer vision, geometric and graph-based microstructure analysis with voxel-based numerical modeling is proposed. Segmented micrographs are processed using the Distance Transform and Watershed algorithms to identify individual fibers and determine their center coordinates. The spatial distribution of fibers is characterized using nearest-neighbor distances, deviations of fiber centers from a reference square lattice, angular distributions, and topological characteristics of spatial graphs. Local spatial order is additionally quantified using fourfold and sixfold bond-orientational order parameters,* ψ_4 *and* ψ_6*. Based on the obtained characteristics, regular and stochastic representative volume element (RVE) models are generated. The stochasticity of the structure is reproduced through controlled random displacement of fiber centers. The proposed approach enables comprehensive quantitative assessment of the heterogeneity of real composite microstructures and provides a basis for generating more realistic composite material models and further investigating their effective mechanical properties.*

Keywords: *fiber-reinforced composites, microstructure, fiber spatial distribution, graph-based analysis, nearest-neighbor distance, stochastic microstructure, representative volume element, voxel modeling, finite element method, computer vision.*

1 Introduction

Fiber-reinforced composites are among the most important modern structural materials and are widely used in aerospace, energy, transportation, and mechanical engineering applications. Their effective mechanical properties are determined not only by the characteristics of their constituents (the matrix and reinforcing fibers) but also by the features of their microstructure, particularly the spatial distribution of fibers within the material. In theoretical and numerical studies, fibers are commonly arranged in regular square or hexagonal arrays. However, experimental investigations and micrograph analyses have shown that real composite materials exhibit deviations from uniformity, including local fiber clustering, regions of increased porosity, and matrix-rich areas, all of which may alter the stress–strain state of the composite [1, 2, 3]. Such non-uniformities are especially common in materials manufactured using filament winding, resin injection molding, and fiber-reinforced additive manufacturing technologies [5]. They lead to variations in local stiffness and redistribution of loads between fibers and the matrix, which in turn affect the macroscopic elastic properties and strength of the structure. Therefore, assessing the

degree of non-uniform fiber distribution is essential for developing more accurate and realistic composite material models and for optimizing their performance.

This study proposes an approach that combines computer vision techniques with numerical modeling for the quantitative analysis of composite microstructures and the evaluation of the influence of non-uniform fiber distribution on the effective material properties. An algorithm was developed to process a set of microstructural image masks of a unidirectional composite, enabling the identification of fiber center coordinates, fiber radii, and deviations from a regular arrangement. Statistical analysis of the processed images is used to determine the average deviation from a regular distribution, which serves as a measure of non-uniformity for subsequent numerical simulations.

Based on the obtained data, a regular voxel-based RVE model and a series of stochastic RVE realizations were generated:

1. A model with a regular fiber distribution;
2. A series of stochastic models with controlled non-uniformity, in which the fiber centers were randomly displaced from their regular positions according to a Gaussian distribution, with a maximum displacement of 15% of the characteristic inter-fiber spacing.

Subsequent simulations make it possible to compare the elastic properties of the two microstructure configurations. This provides a quantitative assessment of the influence of reinforcement non-uniformity on the mechanical behavior of composite materials and establishes a basis for the validation of micromechanical models that account for realistic microstructural features.

2 Related Work

Modeling the mechanical properties of fiber-reinforced composites is traditionally based on the use of representative volume elements (RVEs) and numerical techniques, particularly the finite element method (FEM). This approach enables the determination of effective material properties based on the underlying microstructure. In [5], micromechanical modeling of polymer composites reinforced with basalt and glass fibers was investigated, demonstrating the influence of fiber type and volume fraction on elastic properties. Similar approaches are widely used for evaluating the mechanical behavior of composite materials; however, the microstructure is typically predefined and is rarely analyzed from the perspective of its spatial organization. Analytical methods, particularly the Mori–Tanaka model, remain effective tools for the rapid estimation of composite properties. Recent studies have shown a growing tendency to combine analytical models with numerical simulations and machine learning techniques. In [11], a hybrid approach was proposed in which FEM results were employed to improve the accuracy of an analytical model through machine learning algorithms. This methodology significantly enhances prediction accuracy while maintaining reasonable computational efficiency. An important aspect of composite modeling is the consideration of physical interactions between constituent phases. In [7], the influence of the interphase layer between fibers and the matrix on effective elastic properties was investigated. The study demonstrated that even a thin transition layer can substantially affect the mechanical response of the material, and that the relationships between microstructural parameters and effective properties can be

described using nonlinear regression models. A separate research direction focuses on the generation of stochastic microstructures. In [8], an algorithm for constructing RVEs with randomly distributed particles or fibers was proposed. The method enables the generation of statistically representative microstructures while maintaining a prescribed volume fraction. Statistical descriptors such as nearest-neighbor distances, pair-correlation functions, and Ripley's K-function are commonly employed to quantify the degree of randomness and spatial heterogeneity of the generated structures. Further developments in stochastic modeling have investigated the influence of random generation techniques on simulation results. In [9], it was shown that the choice of random number generation algorithm affects the spatial arrangement of fibers within an RVE, which subsequently influences the statistical characteristics of the predicted mechanical properties. While the average elastic moduli remained relatively stable, significant differences were observed in their variance and distribution. Recent studies have also advanced high-fidelity microstructure modeling techniques. In [10], machine learning methods were applied to generate stochastic RVEs capable of reproducing realistic microstructures of unidirectional composites with high accuracy. Such approaches aim to improve the correspondence between numerical models and actual composite materials. Another important research area concerns the experimental and numerical validation of micromechanical models. In [6], short-fiber composites were investigated using RVE-based homogenization techniques and their averaged variants. The results demonstrated good agreement between numerical predictions and experimental observations. However, the proposed methodology was primarily focused on estimating average material properties rather than analyzing the influence of spatial microstructural heterogeneity. A review of the current literature indicates that most approaches to modeling fiber-reinforced composites are focused on predicting effective average material properties using RVEs, analytical models, or hybrid combinations thereof. Considerable effort has been devoted to improving prediction accuracy and reproducing realistic microstructures. Nevertheless, spatial microstructural characteristics such as inter-fiber distances, local fiber density, and the degree of non-uniform fiber distribution remain insufficiently investigated. Existing approaches generally do not incorporate these factors into the interpretation of simulation results, which limits the ability to fully describe the influence of microstructural heterogeneity on the mechanical behavior of composite materials. Therefore, there is a clear need for methods that combine numerical modeling with quantitative microstructure analysis. In particular, the integration of computer vision techniques with micromechanical modeling provides a promising framework for evaluating spatial heterogeneity and its influence on the effective properties of fiber-reinforced composites.

3 Microstructure Modeling

The microstructure of a fiber-reinforced composite is considered at the level of a representative volume element (RVE), which consists of a matrix and a system of unidirectional fibers with circular cross-sections. Figure 1 illustrates a regular fiber arrangement in which the centers of the inclusions form a periodic lattice with a constant inter-fiber distance *d*.

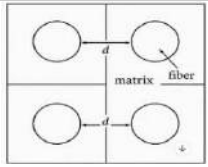


Figure 1. Schematic representation of the regular arrangement of fibers in a composite matrix.

Based on this configuration, a three-dimensional voxel model (Figure 2) of size N × N × N, where N = 40 voxels, is generated. Each element of the domain is assigned a corresponding material phase.



Figure 2. Numerical voxel-based composite model with a regular microstructure: 2D cross-section and 3D representative volume element (RVE) for subsequent FEM analysis.

The selection of the 40×40×40 voxel size is based on the results of a previous study [12], in which the effect of voxel model size on the stability of effective elastic properties was investigated for polycrystalline copper. It was found that increasing the size of the representative volume reduces the statistical scatter of the obtained properties. For a model size of 20 voxels, the mean variance was 1.38, while the maximum deviation of the effective properties did not exceed 1.91%. Based on this observed trend, an RVE size of 40×40×40 voxels was used in the present study as a compromise between the accuracy of microstructure representation and computational cost. Each voxel (x,y,z) is assigned a material phase using the following discrete function:

$$V(x,y,z) = \begin{cases} 1, matrix \\ 2, fiber \end{cases} \quad (1)$$

where the values 1 and 2 are identifiers of the material phases and are used to assign the corresponding physical and mechanical properties within the numerical model. The fiber volume fraction is defined as

$$V_f = \frac{N_{fiber}}{N_{total}} \quad (2)$$

where N_{fiber} - is the number of voxels belonging to the fiber phase, N_{total} - is the total number of voxels in the model.

For the regular fiber arrangement, the fiber volume fraction is determined geometrically through the fiber radius. For stochastic models, the volume fraction is controlled by restricting the displacement of fiber centers and enforcing the non-overlapping condition between fibers.

Stochastic fiber distribution model. To represent the microstructure of real composite materials, which is characterized by deviations from a regular fiber arrangement, a stochastic fiber distribution model is introduced. The model is generated from a regular square packing configuration by applying random displacements to the fiber centers.

The coordinates of the fiber centers $x_i = (x_i, y_i)$ are defined as

$$x_i = x_i^{(0)} + \Delta x_i \quad y_i = y_i^{(0)} + \Delta y_i \tag{3}$$

where $(x_i^{(0)}, y_i^{(0)})$ are the coordinates of the nodes of the regular lattice, and $(\Delta x_i, \Delta y_i)$ are random displacements determined according to a Gaussian normal distribution:

$$\Delta x_i, \Delta y_i \sim N(0, \sigma^2) \tag{4}$$

where σ is a parameter controlling the degree of microstructural heterogeneity.

To ensure the physical validity of the generated microstructure, a non-overlapping condition is imposed on the fibers:

$$\| x_i - x_j \| \geq 2r, i \neq j \tag{5}$$

where r is the fiber radius.

An additional constraint is introduced to limit the maximum displacement of fiber centers, preventing them from leaving their local cells and avoiding excessive distortion of the original structure. The allowable displacement is defined relative to the characteristic cell size and is controlled by a parameter specifying the degree of stochasticity in the fiber distribution. In the present study, the displacement range of the fiber centers was limited to 15% of the characteristic dimension, providing a moderate level of microstructural heterogeneity for the numerical experiments.

This approach enables the generation of microstructures with a controlled degree of non-uniformity, ranging from nearly regular arrangements to significantly random configurations. At the same time, the prescribed fiber volume fraction is preserved, and the condition of geometric non-overlap between fibers is maintained.

The generated stochastic configurations are subsequently used for numerical simulations aimed at investigating the influence of spatial heterogeneity on the effective mechanical properties of composite materials.

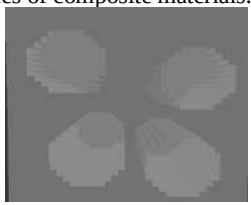


Figure 3. Example of a stochastic composite microstructure generated using Gaussian displacement of fiber centers.

4 Numerical Analysis and Homogenization

To determine the effective mechanical properties of the composite, a numerical analysis of the stress–strain state of the representative volume element (RVE) is performed using the finite element method (FEM).

The mechanical properties of the composite constituents are assigned according to their physical and mechanical characteristics (Table 1). The model consists of two material phases: matrix - isotropic material; fibers - orthotropic material with specified elastic.

Table 1

Mechanical properties of composite constituents

Component	Elastic Properties (GPa)	Poisson's Ratio	Density (kg/m^3)
matrix	$E = 3$	0.35	1200
glass fiber	$E_{33} \approx 76.5$, $E_{11} = E_{22} \approx 10.1$	$\nu_{13} = \nu_{23} \approx 0.22$ $\nu_{12} \approx 0.30$	2650

The stress–strain analysis is carried out within the framework of linear elasticity:

$$\sigma = C\varepsilon \tag{6}$$

where C is the material stiffness tensor determined through the homogenization procedure.

Macroscopic strain components are prescribed as boundary conditions to enforce uniform deformation of the RVE:

$$u(x) = \varepsilon \cdot x \tag{7}$$

where u is the displacement vector; ε is the prescribed macroscopic strain tensor.

All six independent strain components are considered: $\varepsilon_{xx}, \varepsilon_{yy}, \varepsilon_{zz}, \varepsilon_{xy}, \varepsilon_{xz}, \varepsilon_{yz}$.

To construct a complete loading dataset, a combinational loading scheme consisting of 64 loading cases is employed, where each combination corresponds to a separate numerical simulation. For each model, stress and strain fields are obtained and subsequently used to determine the effective material properties through homogenization. The volume-averaged stress and strain tensors are calculated as

$$\langle \varepsilon \rangle = \frac{1}{V} \int_V \varepsilon dV \tag{8}$$

$$\langle \sigma \rangle = \frac{1}{V} \int_V \sigma dV \tag{9}$$

where: ε and σ are the strain and stress tensor components, respectively; $\langle \cdot \rangle$ denotes the volume-averaged value; V is the volume of the representative volume element.

The obtained averaged quantities are used in the homogenization procedure to determine the effective mechanical properties of the composite material.

5 Fiber distribution analysis and microstructure heterogeneity assessment

The input data for the study consist of segmented masks of fiber-reinforced composite cross-sections obtained from micrographs of the material. During data preparation, the reinforcing phase was separated from the matrix and represented as binary images, where each pixel corresponds to one of two phases: fiber or matrix.

To accurately identify individual fibers, a combination of the Distance Transform and the Watershed algorithm is employed. This approach enables the separation of touching or partially overlapping fibers, which is particularly important for composites with a high reinforcement volume fraction. In the first stage, local maxima of the distance function are determined for each fiber region and used as markers for subsequent segmentation. As a result, each fiber is represented as an individual connected component.

For each identified region, its geometric characteristics, including area and centroid coordinates, are determined. In addition, area-based filtering is applied to remove small segmentation artifacts and regions that do not correspond to actual fibers. The coordinates of the centroid of the i-th fiber are calculated as

$$x_i = \frac{1}{A_i}\sum_{k=1}^{A} x_k \quad y_i = \frac{1}{A_i}\sum_{k=1}^{A} y_k \tag{10}$$

where A_i is the area of the *i*-th fiber and (x_k, y_k) are the coordinates of the pixels belonging to the corresponding region.

As a result, a set of fiber center coordinates is obtained:

$$P = \{(x_i, y_i)\}_{i=1}^{N} \tag{11}$$

where N is the total number of fibers in the analyzed cross-section.

The obtained coordinates are used for further analysis of the spatial arrangement of the reinforcing inclusions. Based on these data, inter-fiber distances are calculated, their distributions are analyzed, and the real microstructure is compared with an idealized square-packing model. The resulting statistical characteristics are subsequently used for the generation of stochastic RVE models and for investigating the influence of microstructural heterogeneity on the effective mechanical properties of composite materials. To construct the numerical model, it is necessary to quantify the degree of heterogeneity of the real composite microstructure and determine the allowable displacement of fibers relative to a regular arrangement. A square fiber packing model is adopted as the reference structure since it serves as the basis for the regular RVE model. Using the obtained fiber center coordinates, a regular square lattice with the same number of fibers and the same average center-to-center spacing is generated. For each fiber in the real structure with center coordinates (x_i, y_i), the nearest node of the reference lattice (x_i^0, y_i^0) is identified. The local displacement is then calculated as the Euclidean distance

$$d_i = \sqrt{(x_i - x_i^0)^2 + (y_i - y_i^0)^2} \tag{12}$$

where d_i denotes the displacement of the center of the *i*-th fiber relative to the corresponding reference node.

The resulting set of values characterizes the deviation of the real microstructure from an ideal square packing arrangement. To analyze the local arrangement of fibers, distances to the four nearest neighbors are additionally determined, corresponding to the number of neighboring fibers in a regular square cell. For each fiber, the average nearest-neighbor distance is calculated as

$$L_i = \frac{1}{4}\sum_{k=1}^{4} d_{ik} \tag{13}$$

where d_{ik} is the distance from the center of the i-th fiber to its k-th nearest neighbor.

The mean inter-fiber spacing is then defined as

$$L_{spacing} = \frac{1}{N}\sum_{i=1}^{N} L_i \cdot \tag{14}$$

where N is the number of fibers in the analyzed cross-section.

To construct the reference square lattice, an automatic search is performed for the local microstructural region that most closely resembles a regular square packing arrangement. The selection criterion is based on minimizing the variation of inter-fiber distances and minimizing deviations of the angles between neighboring fibers from 90º. Using the identified cluster, the characteristic inter-fiber spacing and the orientation of the reference structure are determined.

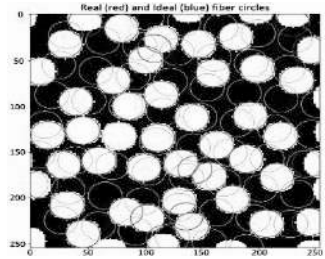


Figure 4. Comparison of the actual fiber arrangement with the regular square packing model.

To evaluate the spatial distribution of fibers, histograms of the average distances to the nearest neighbors were constructed. Unlike hexagonal packing, where each fiber has six nearest neighbors, a square packing arrangement is characterized by four nearest neighbors. Therefore, the primary analysis was performed for k=4.

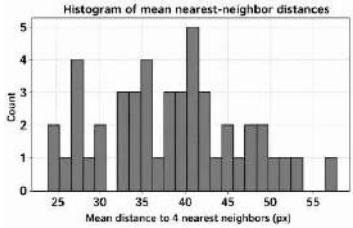


Figure 5. Histogram of the distribution of average distances to the four nearest neighboring fibers.

Figure 5 presents the histogram of the average distances to the four nearest neighboring fibers. The histogram indicates that most fibers exhibit average neighbor distances in the range of 30 – 45 px. The peak of the distribution is located approximately between 38 and 42 px, corresponding to the most characteristic inter-fiber spacing in the analyzed microstructure. At the same time, the finite width of the distribution indicates deviations of the real microstructure from an ideal square packing arrangement and confirms the existence of local regions with increased and decreased fiber density.

Angular and positional analysis. For each detected fiber, the directions toward its nearest neighboring fibers were determined relative to the reference coordinate system. The resulting angular distribution is presented as a polar histogram in Figure 6(a). The angular distribution exhibits pronounced maxima in the directions close to 0◦, 90◦, 180◦, and 270◦. These preferred directions correspond to the principal axes of a square arrangement and indicate the presence of a pronounced fourfold component

in the local organization of the fibers. At the same time, the finite width of the angular peaks and the presence of contributions between the principal directions demonstrate that the experimental structure does not form a perfectly periodic square lattice. Thus, the angular distribution complements the nearest-neighbor distance analysis by demonstrating that local positional variations occur while the predominant fourfold organization of the reference structure is retained.

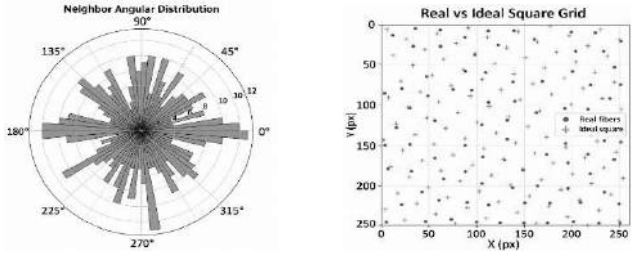


Figure 6. (a) Polar histogram of the angular distribution of nearest neighbors; (b) comparison of the detected fiber centers with the nearest nodes of the ideal square lattice.

Figure 6(b) provides a direct spatial comparison between the experimentally detected fiber centers and the corresponding nearest nodes of the ideal square lattice. The observed displacements vary throughout the analyzed cross-section: some fibers remain close to their reference positions, whereas others exhibit more pronounced deviations. This spatial variation demonstrates that the microstructure contains local positional fluctuations while maintaining the overall organization associated with the square reference configuration.

The positional and angular descriptors therefore provide complementary information. The displacement from the reference lattice characterizes the deviation of individual fiber positions, whereas the angular distribution describes the preservation of preferred local orientations. Their combination provides a more complete description of the spatial heterogeneity of the experimental microstructure.

Graph-based representation of fiber spatial arrangement. To additionally characterize the local organization of the reinforcing phase, the fiber centers were represented as vertices of a spatial graph, with edges defining the corresponding neighborhood relationships. The graph representation makes it possible to quantify not only the distances between fibers but also the number and organization of neighboring fibers. Three complementary graph constructions were considered. First, a Delaunay graph was generated from the fiber center coordinates and used as a baseline geometrical representation. This construction defines spatial connectivity directly from the distribution of the fiber centers without requiring a predefined maximum neighborhood distance. For the analyzed microstructure containing 87 fibers, the Delaunay graph contained 247 edges. The mean number of neighboring fibers was 5.68, with a median of 6. The minimum and maximum numbers of neighbors were 4 and 8, respectively. The lengths of the Delaunay edges were also analyzed. The mean edge length was 36.18 px, while the median was 30.05 px and the standard deviation was 19.72 px. The edge lengths ranged from 17.71 to 164.33 px. The difference between the mean and median values, together with the presence of relatively long edges, indicates that the Delaunay graph includes both locally close

fibers and comparatively long geometrical connections. To account for differences in fiber size, the center-to-center distance was normalized by the combined radii of the corresponding fibers:

$$R_{ij} = \frac{d_{ij}}{r_i + r_j}, \tag{15}$$

where d_{ij} is the center-to-center distance and r_i and r_j are the equivalent radii of fibers i and j respectively.

For the analyzed Delaunay graph, the mean normalized distance was 1.54 and the median was 1.25. The 75th, 90th and 95th percentiles were 1.64, 2.29 and 3.32, respectively, while the maximum value was 7.16. The obtained distribution indicates that not all Delaunay connections represent immediate local fiber proximity. Therefore, a distance-filtered Delaunay graph was additionally considered. An edge was retained when its normalized distance did not exceed $R_{\max} = 2.0$. This threshold was used as a controlled parameter for sensitivity analysis of the neighborhood definition rather than as a universal physical criterion.

After filtering, the number of edges decreased from 247 to 215 and the mean degree decreased from 5.68 to 4.94. The median degree was 5, while the minimum and maximum degrees were 2 and 8, respectively. No isolated fibers were obtained.

As a third representation, a Gabriel graph was constructed from the same fiber center coordinates. In this case, a Delaunay connection was retained when the circle defined by the corresponding center-to-center segment as its diameter contained no other fiber center. This provides a local geometrical neighborhood definition without requiring an explicitly selected distance threshold. The Gabriel graph contained 190 edges. Its mean degree was 4.37 and the median degree was 4, with a standard deviation of 1.16. The minimum and maximum degrees were 1 and 7, respectively, and no isolated fibers were detected. The characteristics of the three graph representations are summarized in Table 2. The comparison demonstrates that the estimated local connectivity depends on the definition of spatial neighborhood. The Delaunay graph provides the largest number of geometrical connections, while the distance-filtered graph removes part of the longer connections according to the selected normalized-distance criterion. The Gabriel graph provides a more restrictive local neighborhood representation without introducing an empirical distance threshold.

Table 2

Topological characteristics of the investigated fiber spatial graphs

Parameter	Delaunay	Delaunay, $R_{ij} \le 2.0$	Gabriel
Number of fibers	87	87	87
Number of edges	247	215	190
Mean degree	5.68	4.94	4.37
Median degree	6	5	4
Standard deviation	—	—	1.16
Minimum degree	4	2	1
Maximum degree	8	8	7

The three approaches were therefore treated as complementary descriptors of the fiber arrangement. The Delaunay graph characterizes the geometrical connectivity of the complete center distribution, the filtered Delaunay graph evaluates the effect of a controlled proximity criterion, and the Gabriel graph provides a parameter-free representation of local geometrical neighborhoods.

Local spatial order. The angular organization of neighboring fibers was further quantified using local bond-orientational order parameters. For the i-th fiber, the fourfold and six fold components of the local spatial arrangement were calculated as

$$\psi_4(t) = \left| \frac{1}{N_i} \sum_{j \in N_i} \exp(4i\theta_{ij}) \right|. \quad (16)$$

$$\psi_6(t) = \left| \frac{1}{N_i} \sum_{j \in N_i} \exp(6i\theta_{ij}) \right|. \quad (17)$$

where N_i is the number of neighboring fibers, N_i is the corresponding neighborhood, and θ_{ij} is the angular position of neighboring fiber j relative to fiber i.

The parameter ψ_4 characterizes the local fourfold orientational component, whereas ψ_6 characterizes the sixfold component. Values approaching unity indicate stronger angular coherence with the corresponding symmetry. The corresponding median values were 0.3253 and 0.4865, with standard deviations of 0.2365 and 0.2500, respectively. The higher mean and median values of ψ_6 compared with ψ_4 indicate a stronger sixfold component according to the local bond-orientational descriptor. However, this result does not imply that the entire microstructure has a globally hexagonal arrangement. Rather, it indicates that local fiber neighborhoods contain a measurable sixfold orientational component in addition to the dominant square-like organization observed in the angular distribution.

The relatively large standard deviations of the local order parameters demonstrate that the degree of orientational organization varies between individual fiber neighborhoods. Thus, the local order parameters provide information about spatial heterogeneity that cannot be obtained from a single global descriptor.

Quantification of microstructural heterogeneity. The combined analysis of fiber positions, inter-fiber distances, angular distribution and local neighborhood topology demonstrates that the investigated microstructure retains a predominantly square-like organization while exhibiting local spatial variations.

For the analyzed microstructure, the mean nearest-neighbor distance was 23.53 px, with a median of 23.82 px and a standard deviation of 2.38 px. The coefficient of variation was 10.10%, indicating moderate variability in local fiber spacing. The angular distribution further confirmed the presence of preferred directions corresponding to the principal axes of the square packing, while the comparison with the ideal lattice demonstrated local positional deviations of the fiber centers.

The graph-based and local orientational analyses additionally revealed variations in the number and angular organization of neighboring fibers. Thus, the observed heterogeneity is manifested not only through variations in inter-fiber spacing but also through local positional and topological differences.

These characteristics were used to define the degree of stochasticity of the generated RVE models. To reproduce the observed deviations from the regular square arrangement, the fiber centers were randomly displaced according to a Gaussian distribution. Based on the obtained spatial statistics and preliminary numerical experiments, the maximum displacement was limited to 15% of the characteristic inter-fiber spacing. This value provides moderate positional variability while preserving the predominant square-like organization, the prescribed fiber volume fraction, and the non-overlapping condition between fibers.

The resulting stochastic configurations were subsequently used for numerical simulations of the effective mechanical properties of the composite material.

6 Result and Discussion

To investigate the influence of spatial microstructural heterogeneity on the effective mechanical properties of the composite, a series of stochastic models was generated by randomly displacing the fiber centers relative to a regular square lattice. To obtain statistically stable estimates of the effective mechanical properties, 100 independent stochastic realizations were generated. This number of realizations provides a more accurate estimation of the mean mechanical properties, reduces the influence of random deviations in individual realizations, and allows for a more representative characterization of the statistical distribution of the composite properties. For each realization, a homogenization procedure was performed to determine the effective elastic moduli, shear moduli, and Poisson's ratios.

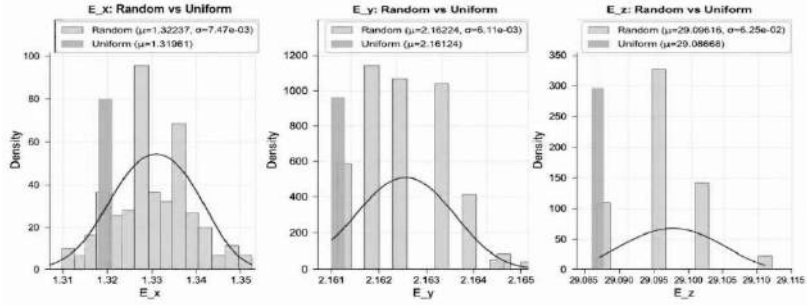


Figure 7. Statistical distributions of the effective elastic moduli for random and uniform fiber distributions.

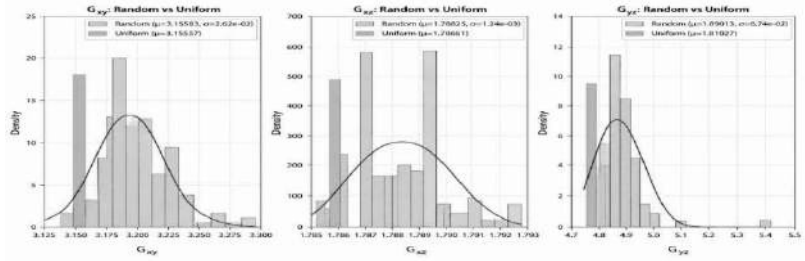


Figure 8. Statistical distributions of the effective shear moduli for random and uniform fiber distributions.

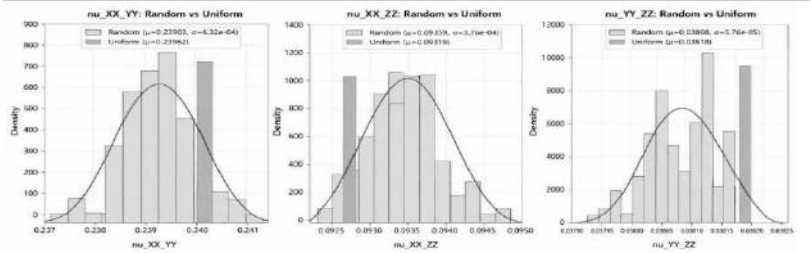


Figure 9. Statistical distributions of the effective Poisson's ratios for random and uniform fiber distributions.

Figures 7–9 present the histograms of the effective properties obtained for the stochastic microstructures. The blue bars correspond to the results of individual realizations with randomly distributed fibers, while the blue curves represent approximations using a normal probability distribution. The orange bars indicate the corresponding values obtained for the regular model with a symmetric fiber arrangement. Analysis of the histograms shows that the distributions of most effective mechanical properties are close to normal. Furthermore, the values obtained for the regular model are located near the centers of the corresponding distributions. This indicates that random displacements of fiber centers do not significantly affect the average mechanical properties of the composite. However, they introduce a measurable statistical variation in the predicted effective properties, reflecting the influence of microstructural heterogeneity on the material response. For a quantitative assessment of the obtained distributions, the main statistical characteristics of the effective elastic properties are presented in Table 3. The table includes the mean value μ, the standard deviation σ, and the coefficient of variation CV, which is defined as

$$CV = \frac{\sigma}{\mu} \cdot 100\% \cdot \tag{18}$$

Table 3

Statistical characteristics of effective elastic properties for stochastic composite microstructures

Property	Regular Mode	Mean Value (μ)	Standard Deviation (σ)	CV, %
E_x, (GPa)	4.320	4.327	0.0075	0.17
E_y, (GPa)	2.461	2.462	0.0008	0.03
E_z, (GPa)	29.087	29.096	0.0063	0.02
G_xy, (GPa)	3.156	3.186	0.0262	0.82
G_xz, (GPa)	1.787	1.788	0.0012	0.07
G_yz, (GPa)	4.840	4.890	0.0674	1.38
ν_xy	0.2396	0.2390	0.00063	0.26
ν_xz	0.0932	0.0936	0.00038	0.40
ν_yz	0.0382	0.0381	0.00006	0.15

The coefficient of variation provides a measure of the relative dispersion of the results independently of the absolute magnitude of the considered parameter. Higher

values of CV indicate greater sensitivity of the corresponding mechanical property to the random spatial distribution of fibers within the composite matrix. To quantitatively assess the influence of stochastic fiber arrangement on the effective mechanical properties of the composite, the homogenization results obtained for the regular and stochastic models were compared.

Table 4 presents the effective elastic moduli and shear moduli calculated for both types of microstructures, together with the relative deviation between them:

$$\Delta P = \frac{|P_{ran} - P_{reg}|}{P_{reg}} \cdot 100\%, \quad (19)$$

where P_{reg} and P_{ran} denote the effective property obtained for the regular and stochastic microstructures, respectively.

Table 4

Comparison of effective elastic and shear moduli for regular and stochastic composite models.

Property	$P_{regular}$ **(GPa)**	P_{random} **(GPa)**	ΔP **(%)**
E_x	4.319	4.327	0.19
E_y	2.461	2.462	0.04
E_z	29.09	29.10	0.03
G_{xy}	3.155	3.186	0.98
G_{yz}	4.840	4.890	1.03
G_{xz}	1.787	1.788	0.06

As shown in Table 4, the mean values of the effective properties obtained for the stochastic models remain close to those of the regular microstructure. The largest deviation is observed for the shear modulus G_{yz} however, even in this case the difference does not exceed 1.1%. For the elastic moduli E_x, E_y, and E_z, the deviations are below 0.2%, indicating that the average stiffness of the material is largely preserved despite the random displacement of fiber centers. These results suggest that moderate microstructural heterogeneity has only a limited effect on the mean effective mechanical properties of the composite. Nevertheless, as demonstrated by the statistical analysis presented in Table 4, stochastic fiber distributions introduce a measurable variability in the predicted properties, which should be considered when assessing the reliability and uncertainty of composite material performance Table 5 presents a comparison of the effective Poisson's ratios obtained for the regular and stochastic composite microstructures. Similar to the elastic and shear moduli, the calculated values exhibit only minor differences between the two models. The close agreement between $v_{regular}$ and v_{random} indicates that the random spatial distribution of fibers does not significantly affect the macroscopic deformation behavior of the composite material. These results confirm that moderate microstructural heterogeneity has a negligible influence on the effective Poisson's ratios, while the overall elastic response of the composite remains governed primarily by the constituent material properties and the fiber volume fraction.

Table 5

Comparison of effective Poisson's ratios for regular and stochastic composite models

Property	$\nu_{regular}$	ν_{random}
$\nu_{x,y}$	0.2396	0.2390
$\nu_{x,y}$	0.0932	0.0936
$\nu_{x,y}$	0.0382	0.0381

Conclusions

This study investigated the influence of non-uniform fiber distribution on the effective elastic properties of a unidirectional fiber-reinforced composite using a combination of image-based microstructure analysis and voxel-based numerical modeling. A methodology was developed to characterize the spatial organization of fibers from segmented micrographs and to use the obtained characteristics for the construction and evaluation of stochastic representative volume element (RVE) models. The analysis of the experimental microstructure demonstrated that the fiber arrangement retains a predominantly square-like organization while exhibiting local deviations in fiber positions and inter-fiber spacing. For the analyzed microstructure, the mean nearest-neighbor distance was 23.53 px, with a median of 23.82 px and a coefficient of variation of 10.10%. The angular distribution showed pronounced preferred directions close to 0◦, 90◦, 180◦, and 270◦, confirming the presence of a dominant fourfold component while also demonstrating deviations from an ideal periodic arrangement.

The graph-based analysis provided an additional quantitative description of the local fiber neighborhoods. Three spatial representations were compared: the Delaunay graph, a distance-filtered Delaunay graph, and the Gabriel graph. For the analyzed microstructure, the corresponding mean numbers of neighboring fibers were 5.68, 4.94, and 4.37, respectively. The comparison demonstrated that the estimated local connectivity depends on the definition of spatial neighborhood. The Delaunay graph provides a general geometrical representation, while the distance-filtered and Gabriel graphs provide more localized descriptions of fiber proximity. The local bond-orientational parameters further characterized the angular organization of individual neighborhoods, with mean values of. ψ_4 = 0.3711 and ψ_6 = 0.5168 for the Gabriel graph. The obtained microstructural characteristics were used to support the construction of stochastic RVE models. The stochastic fiber distribution was generated by randomly displacing fiber centers relative to a regular square lattice according to a Gaussian probability distribution. The maximum displacement was limited to 15% of the characteristic inter-fiber spacing in order to introduce moderate spatial variability while preserving the general organization of the fiber arrangement and preventing geometric overlap.

The numerical results demonstrated that the introduction of spatial heterogeneity has a minor effect on the mean effective elastic properties of the investigated composite. For the elastic moduli, the maximum deviation between the regular and stochastic models was less than 0.2% for E_x , 0.04% for E_y , and 0.03% for E_z . For the shear moduli, the deviations did not exceed 1.03%. The largest changes were

observed for $G_{x,y}$ and $G_{y,z}$, for which the relative increases reached 0.98% and 1.03%, respectively. The differences in Poisson's ratios remained below 0.5%. At the same time, stochastic configurations introduced a statistical variability of the effective mechanical properties that was absent in the regular model. Thus, although the spatial heterogeneity considered in this study has a limited influence on the mean effective properties, it affects the statistical distribution of the numerical results. This distinction is important when the objective is not only to estimate average material properties but also to characterize their variability and the influence of local microstructural features. For the investigated composite with a fiber volume fraction of 40% and a maximum fiber displacement of 15%, the regular RVE model provides a close estimate of the mean effective elastic properties. However, stochastic RVE models are more appropriate when the analysis requires consideration of the variability of mechanical properties, local microstructural effects, or statistical reliability. The proposed combination of image-based spatial characterization, graph-based analysis, and stochastic RVE generation can therefore be used as a basis for developing more representative computational models of heterogeneous fiber-reinforced composites.

Acknowledgements

The authors acknowledge the support of the Ministry of Education and Science of Ukraine through the research project “Algorithms, Models, and Artificial Intelligence Tools for Two-Level Modeling of the Behavior of Complex Materials for Dual-Use Applications” (State Registration No. 0124U000450).

References

[1] W. Wang, Y. Dai, C. Zhang, X. Gao, and M. Zhao, Micromechanical Modeling of Fiber-Reinforced Composites with Statistically Equivalent Random Fiber Distribution, Materials, vol. 9, no. 8, Art. no. 624, 2016, doi:10.3390/ma9080624.

[2] A. P. Chatterjee, Nonuniform Fiber Networks and Fiber-Based Composites: Pore Size Distributions and Elastic Moduli, Journal of Applied Physics, vol. 108, no. 6, Art. no. 063513, 2010, doi:10.1063/1.3485823.

[3] S. Qi, O. Alajarmeh, M. Alhawamdeh, T. Shelley, P. Schubel, K. Rendle-Short, and X. Zeng, Formation of Non-Uniform Fibre Distribution and Its Effect on the Flexural Performance of Pultruded GFRP Box Beams, Composite Structures, vol. 327, Art. no. 117695, 2024, doi:10.1016/j.compstruct.2023.117695.

[4] M. Mehdikhani, L. Gorbatikh, I. Verpoest, and S. V. Lomov, Voids in Fiber-Reinforced Polymer Composites: A Review on Their Formation, Characteristics, and Effects on Mechanical Performance, Journal of Composite Materials, vol. 53, no. 12, pp. 1579–1669, 2019, doi:10.1177/0021998318772152.

[5] F. Yildirim, Micromechanical Modeling of Basalt Fiber and Glass Fiber Reinforced PA66 Matrix Composite Materials, Uludağ University Journal of the Faculty of Engineering, vol. 30, no. 1, pp. 87–106, Apr. 2025, doi:10.17482/uumfd.1557584.

[6] M. G. Andika, T. S. Nurtiasto, K. Abdurohman, A. R. Hidayat et al., Optimized Mori–Tanaka Model with FEM-RVE Corrections and Machine Learning for High-Fidelity Composite Mechanical Property Estimation, Mar. 2025, doi:10.21203/rs.3.rs-6266841/v1.

[7] Y. Liu, Y. Yan, L. Yang, M. He et al., Prediction on Macroscopic Elastic Properties of Interphase-Contained Long-Fiber-Reinforced Composites and Multiple Nonlinear Regression Analysis, Journal of Reinforced Plastics and Composites, vol. 31, no. 17, pp. 1143–1157, Sep. 2012, doi:10.1177/0731684412454461.

[8] A. R. Melro, P. P. Camanho, and S. T. Pinho, Generation of Random Distribution of Fibres in Long-Fibre Reinforced Composites, Composites Science and Technology, vol. 68, no. 9, pp. 2092–2102, 2008, doi:10.1016/j.compscitech.2008.03.013.

[9] B. Rajjoub and C. Balzani, On the Role of Random Number Generation Algorithms in the Micromechanical Modeling of Fiber Composites, IOP Conference Series: Materials Science and Engineering, vol. 1338, no. 1, Art. no. 012013, Oct. 2025, doi:10.1088/1757-899X/1338/1/012013.

[10] C. Ji, Y. Zhai, D. Li, and H. Qu, High-Fidelity Modeling of Stochastic RVE Based on Learning Strategies for Unidirectional Fiber Reinforced Composite Material, Polymer Composites, vol. 47, no. 12, pp. 11256–11275, Mar. 2026, doi:10.1002/pc.71018.

[11] W. A. Moussa, Y. S. Mohamed, and A. Abdelbary, Finite-Element Homogenization of Short Glass Fiber/Silicone Rubber Composites: Experimental Validation of RVE and Orientation-Averaged RVE Methods, Journal of Reinforced Plastics and Composites, Dec. 2025, doi:10.1177/07316844251409846.

[12] V. Zhykhariev, M. Shapovalova, O. Vodka, S. Misiura, Numerical Study of the Size Effect and Nucleation Center Concentration on the Elastic Properties of Copper, Scientific Journal of the Ternopil National Technical University, vol. 121, no. 1, 2026. doi:10.33108/visnyk_tntu2026.01.020.

ВОКСЕЛЬНЕ МОДЕЛЮВАННЯ ВПЛИВУ НЕРІВНОМІРНОГО РОЗПОДІЛУ ВОЛОКОН НА ЕЛАСТИЧНІ ВЛАСТИВОСТІ ВОЛОКОНОЗМІЦНЕНИХ КОМПОЗИТІВ

Ph.D., Водка О., Ph.D., Шаповалова М., Ph.D., Місюра С., Жихарієв В.
Національний технічний університет «Харківський політехнічний інститут», Україна

Анотація. *У цій статті досліджується вплив просторової неоднорідності розподілу волокон на мікроструктурні характеристики та ефективні пружні властивості однонаправлених волокнистих композитів. Запропоновано комплексну методологію, що поєднує комп'ютерний зір, геометричний та графовий аналіз мікроструктури з воксельним чисельним моделюванням. Сегментовані мікрофотографії обробляються за допомогою алгоритмів «Distance Transform» та «Watershed» для ідентифікації окремих волокон та визначення координат їхніх центрів. Просторовий розподіл волокон характеризується за допомогою відстаней до найближчих сусідів, відхилень центрів волокон від еталонної квадратної решітки, кутових розподілів та топологічних характеристик просторових графів. Локальний просторовий порядок додатково кількісно оцінюється за допомогою чотирикратних та шестикратних параметрів орієнтаційного порядку зв'язків, та . На основі отриманих характеристик генеруються регулярні та стохастичні моделі репрезентативних об'ємних елементів (RVE). Стохастичність структури відтворюється за допомогою контрольованого випадкового зміщення центрів волокон. Запропонований підхід дає змогу провести комплексну кількісну оцінку неоднорідності реальних мікроструктур композитів та забезпечує основу для побудови більш реалістичних моделей композиційних матеріалів і подальшого дослідження їхніх ефективних механічних властивостей.*

Ключові слова: *композитні матеріали, армовані волокнами, мікроструктура, просторовий розподіл волокон, аналіз на основі графів, відстань до найближчого сусіда, стохастична мікроструктура, репрезентативний об'ємний елемент, воксельне моделювання, метод скінченних елементів, комп'ютерний зір.*

UDC 621.396.946:004.056
DOI

LORAWAN IN AVIATION: A COMPREHENSIVE ANALYSIS OF CYBER THREATS AND RESILIENCE STRATEGIES

Tertus Y.[0009-0004-8861-6092], Kozlovska D.[0009-0004-6223-0319],
Dr.Sci., Kozlovsky V.[0000-0002-8301-5501], Kotyk B.[0009-0005-0821-9108]
State University "Kyiv Aviation Institute", Ukraine
EMAIL: 4142569@stud.kai.edu.ua

Abstract. *The rapid development of aviation cyber-physical infrastructures, including smart airport systems, unmanned aerial platforms, and distributed telemetry environments, increases the importance of communication technologies that can simultaneously ensure long-range coverage, low power consumption, and acceptable resilience under dynamic operational conditions. LoRaWAN is considered one of the most promising LPWAN technologies for such scenarios due to its Chirp Spread Spectrum physical layer, star-of-stars architecture, and suitability for sparse autonomous sensing systems [10]. At the same time, aviation use imposes stricter requirements on communication continuity, integrity, latency, cyber resilience, and assurance than conventional IoT applications, which means that direct adoption of LoRaWAN without adaptation is unsafe and methodologically unjustified. This article expands the original review into a full scientific study based primarily on the same reference base already present in the source manuscript. The paper systematizes technological properties of LoRa/LoRaWAN in aviation systems, analyzes the principal deployment scenarios, formalizes a multi-layer threat model, compares methods for improving interference immunity and cyber resilience, and proposes an integrated framework for aviation-oriented adaptation of LoRaWAN infrastructures. In addition, the proposed framework is evaluated through a MATLAB-based Monte Carlo simulation of airport-support telemetry under normal operation and reactive jamming, demonstrating improved packet delivery, attack detectability, and post-attack recovery. The overall objective is to provide a structured conceptual basis for designing, evaluating, and further researching aviation LoRaWAN networks under realistic constraints of interference, mobility, and cyber threat exposure.*

Keywords: *LoRaWAN, Cyber Security, Interference Immunity, Artificial Intelligence, Data Processing, Machine Learning*

1 Introduction and Research Background

1.1 Relevance of LoRaWAN for aviation applications

The aviation sector is undergoing a phase of intensive digital transformation driven by distributed sensing, autonomous unmanned systems, smart airport infrastructure, remote monitoring, and the broader integration of Internet of Things concepts into operational and support environments. These processes increase the need for communication systems capable of serving geographically dispersed nodes under power constraints, mobility, and adverse radio conditions while maintaining acceptable reliability and security. LoRaWAN occupies a visible place among LPWAN technologies because it combines long com-munication range, low energy consumption, and relatively simple deployment, making it attractive for environmental sensing, maintenance telemetry, perimeter monitoring, mobile data collection, and UAV-assisted communications. In aviation-oriented applications, these properties are especially relevant where cellular connectivity is unavailable, expensive, or inadequate for long-duration autonomous operation.

1.2 Research problem and limitations of direct LoRaWAN adoption in aviation

However, LoRaWAN was not originally designed for critical aviation contexts. The protocol inherits a number of vulnerabilities at the PHY, MAC, network, and cryptographic levels, especially in older versions and weak implementations, which makes it sensitive to selective jamming, replay attacks, wormhole manipulation, rogue gateways, battery depletion, and device compromise. In aviation systems, such attacks may affect not only data confidentiality but also telemetry integrity, control continuity, maintenance awareness, and mission coordination.

1.3 Aim, objectives, and scientific contribution of the article

The objectives are: to deepen the literature review, clarify technological properties of LoRa/LoRaWAN in aviation systems, systematize aviation use cases, formalize a threat model, compare methods of improving resilience, analyze FANET-specific issues, address certification and regulatory constraints, and propose an integrated framework for future research and engineering design [1, 2, 6, 8, 12]. The scientific novelty of this work lies in the integration and quantitative validation of a cross-layer re-silience framework for aviation-support LoRaWAN telemetry. Unlike studies that consider anti-jamming techniques, gateway diversity, intrusion detection, or recovery mechanisms separately, the proposed approach combines these mechanisms into a single monitoring–assessment–adaptation–recovery con-trol loop. The framework is evaluated through a reproducible Monte Carlo simulation that compares a static LoRaWAN baseline with an adaptive multi-gateway configuration under reactive jamming. The results quantify the resulting gains in packet delivery, jamming resilience, attack detection, and recovery performance. The remainder of the paper distinguishes background material from the authors' original contribution. Sections 2–4 summarize the technological foundations, aviation use cases, threat landscape, and existing resilience methods. Section 5 presents the authors' integrated cross-layer framework and its control logic. Section 5.5 provides the original simulation-based validation and quantitative comparison with a static baseline configuration. Section 6 discusses limitations, implementation boundaries, and future research directions.

2 Technological Foundations of LoRaWAN in Aviation

2.1 Physical-layer characteristics of LoRa and their aviation relevance

LoRa and LoRaWAN should be analyzed separately because their contribution to aviation suitability differs by layer. LoRa is the physical-layer technology based on Chirp Spread Spectrum modulation, while LoRaWAN defines the network architecture, activation procedures, device classes, session management, and backend trust relations [10, 12]. In aviation, this distinction matters because radio robustness and protocol security do not automatically imply one another.

The physical layer of LoRa provides high receiver sensitivity and supports communication over large distances with low transmit power. One of the most important factors is the spreading factor, which determines the degree of spreading and directly affects sensitivity, airtime, and throughput. This can be expressed through the symbol duration formula:

$$T_s = \frac{2^{SF}}{BW} \quad (1)$$

where T_s is symbol duration, SF is the spreading factor, and BW is bandwidth. This relation shows that increasing SF improves range and resistance to path loss, but also significantly increases transmission time and vulnerability exposure window.

A simplified frame airtime expression may be written as:

$$T_{frame} \approx T_{preamble} + N_{sym} \cdot T_s, \quad (2)$$

where N_{sym} is the effective number of payload-related symbols. In aviation networks, longer airtime is a double-edged property: it can support difficult links, but also increases latency and makes reactive jamming more effective [10, 14, 15, 16].

2.2 LoRaWAN architecture, device classes, activation logic and operational constraints

LoRaWAN implements a star-of-stars model in which end devices communicate with gateways, gate-ways forward traffic to network servers, and backend services handle activation and application-level delivery. This architecture is deployment-friendly and scales well for low-rate sensing, but it also creates dependencies on gateway authenticity, backend trust, and secure join procedures. In aviation applications, such dependencies become especially important because gateways may be mobile, remotely deployed, or physically exposed [6, 10, 12].

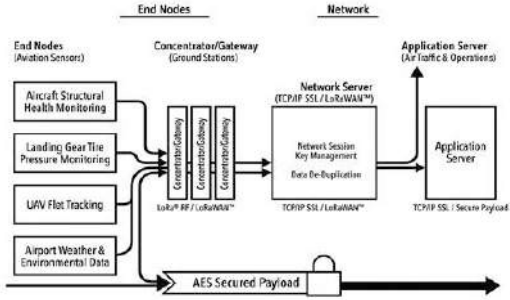


Figure 1. LoRaWAN Protocol Architecture

LoRaWAN device classes determine how often nodes can receive downlink traffic and therefore affect energy consumption and responsiveness. For long-life airport sensors, lower-power behavior may be acceptable, while UAV-oriented scenarios may require more responsive classes despite higher energy costs. Activation procedures also matter. Over-the-Air Activation supports dynamic onboarding and session re-establishment, whereas static personalization approaches may reduce flexibility after compromise or redeployment [10, 12]. In aviation applications, radio robustness and protocol security do not automatically imply one another. Longer airtime can support difficult links but also increases latency and vulnerability exposure, gateway authenticity and backend trust remain critical because gateways may be mobile or physically exposed, and the choice of device classes creates a trade-off between responsiveness and energy consumption [6, 10, 12, 14, 15, 16]. Overall, LoRaWAN 1.1 should be regarded as the minimum security baseline for aviation-oriented deployments, although further protective mechanisms remain necessary [12, 20].

3 Aviation Applications and Threat Landscape

3.1 Main aviation use cases: airport monitoring, telemetry, tracking, degraded-mode communications

The practical significance of LoRaWAN in aviation depends on the specific operational scenario. A protocol that is acceptable for autonomous environmental sensing may be unsuitable for low-latency control-related exchange. Therefore, the deployment context must be analyzed explicitly [6]. In airport environments, LoRaWAN can be used for perimeter sensors, runway lighting diagnostics, weather stations, vibration sensing, environmental monitoring, equipment tracking, and support telemetry. Such applications are attractive because they reduce installation costs, support autonomous sensors, and can operate over large aerodrome areas without full wired infrastructure. [6, 10, 15].

Table 1

Comparison of LPWAN technologies for aviation applications

Criterion	LoRaWAN	NB-IOT	LTE-M	Sigfox
Spectrum	Unlicensed ISM	Licensed cellular	Licensed cellular	Unlicensed ISM
Infrastructure dependence	Private or public gateways	Cellular operator network	Cellular operator network	Sigfox network availability
Typical data capability	Low-rate telemetry	Low-rate telemetry	Moderate-rate telemetry and mobility support	Very-low-rate messaging
Energy efficiency	High for sparse periodic sensing	High, but network attachment may increase overhead	Moderate	Very high for small payloads
Mobility suitability	Limited in standard static deployments	Limited to moderate	Better than other LPWAN options	Limited
Private deployment control	High	Low to moderate	Low to moderate	Low
Aviation-support suitability	Strong for private airport sensing, monitoring, and degradedmode telemetry	Suitable where cellular coverage and operator integration are acceptable	Suitable for more mobile, latency-sensitive support applications	Suitable only for sparse, non-critical messages
Main limitation	Non-deterministic access; unlicensedband interference; assurance	Dependency on cellular infrastructure and subscription	Energy and cost overhead	Payload, downlink, and coverage limitations

LoRaWAN is well suited for low-rate telemetry and asset tracking, particularly where power economy and communication range are more important than throughput. However, even in these scenarios, strict protection against spoofing, stale data, and replay remains necessary if the information contributes to operational decision-making [6, 10]. Aviation systems often rely on layered architectures. In this context, LoRaWAN may be highly effective as a degraded-mode or backup communication channel rather than as the sole communication backbone. This use model is consistent with the article's recommendation to combine LoRa with LTE, 5G, or other backup paths when continuity and trusted recovery are critical [6].

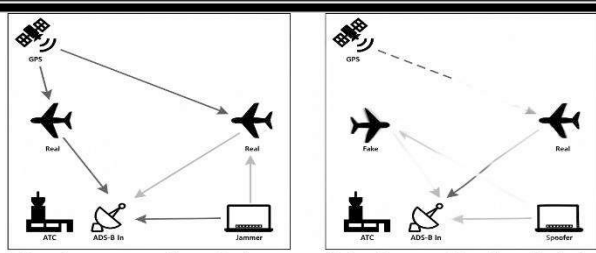
No LPWAN technology should be regarded as universally optimal for aviation applications. LoRaWAN offers a strong combination of private deployment control, low power consumption, and wide-area sensing capability, which is attractive for airport-support telemetry. NB-IoT and LTE-M can provide advantages where licensed spectrum, operator-managed coverage, and cellular integration are available, while LTE-M is generally more suitable for mobility-oriented support applications. Sigfox is appropriate only for sparse and non-critical messaging because of its constrained payload and downlink capability. None of these technologies should be considered a direct replacement for certified safety-critical aviation communication systems.

3.2 UAVs and FANET-based deployment scenarios

One of the most promising use cases is the use of unmanned aerial vehicles as mobile gateways collecting data from ground sensors or disconnected devices. Such architecture can support emergency monitoring, search-and-rescue support, temporary infrastructure restoration, and wide-area environmental sensing. Its advantages are rapid deployment, geometric flexibility, and ability to service difficult terrain. At the same time, UAV gateways create new risks. Airborne nodes may be jammed, captured, imitated, or geospatially targeted. Since they often act as concentration points between distributed sensors and backend systems, compromise of a UAV gateway may have disproportionate operational effects [6, 13]. Flying Ad Hoc Networks are attractive because they can support distributed coordination among UAVs with low-energy communications [13]. However, FANETs are also among the most challenging environments for LoRaWAN because standard protocol assumptions do not include dynamic mesh-style topology, relay trust, or fast re-authentication during topology changes. This mismatch is one of the most important scientific challenges identified in the article.

3.3 Threat model for LoRaWAN-based aviation networks

The original article already contains a valuable threat taxonomy, but a full-length paper should make the threat model more explicit by linking attack mechanisms to operational consequences [6]. In aviation contexts, threats must be evaluated not only by technical possibility but also by mission effect. Potential adversaries include passive observers, active RF attackers, insider threats, technically skilled external actors, and adversaries targeting disruption rather than data theft. Some attackers may only observe traffic and infer patterns, while others may inject, replay, tunnel, jam, or physically compromise nodes. In aviation environments, even a modest attacker can become operationally dangerous if the system depends on continuity and trusted telemetry [5, 6, 15].



(a) Jamming: prevent or disrupt signal reception from the ADS-B receiver or the GPS.

(b) Spoofing: transmitting fake radio signals to deceive either the ADS-B receiver or the GPS.

Figure 2. Jamming and Spoofing cyberattacks on flight safety

3.4 Mission impact of PHY, MAC, network, and hardware-level attacks

Selective jamming and reactive jamming are among the most severe LoRa-related attacks because they directly target availability [14, 15, 16]. A simplified availability relation can be written as:

$$A = 1 - P_{loss} \tag{3}$$

where P_{loss} is packet loss probability due to noise, interference, collisions, or active jamming. Un-der hostile conditions, this probability becomes dependent on link parameters, jammer timing, and infrastructure diversity [15, 16].

A more explicit conceptual dependency may be represented as:

$$P_{loss} = f(SF, BW, J, D, C) \tag{4}$$

where J denotes jammer effectiveness, D gateway diversity, and C channel congestion. This is useful because it shows that availability is not only a radio-quality issue but a resilience issue shaped by architecture and attack pressure [14, 16].

Replay attacks exploit old valid frames and are especially dangerous when stale telemetry or repeated commands can influence operations. Wormhole attacks distort topology and timing by tunneling traffic, thereby affecting geolocation, trust relationships, or route assumptions. Rogue gateways are similarly dangerous because they can relay, delay, or manipulate traffic while appearing legitimate to poorly protected infrastructure [5, 6, 12].

4 Methods for Improving Resilience

4.1 Methods for improving interference immunity: adaptive parameters, hopping, gateway diversity, UAV relays

The original article correctly identifies adaptive transmission, gateway diversity, relays, hybrid archi-tectures, and frequency agility as the principal methods for improving interference immunity. In this expanded version, these methods are interpreted more systematically. Adaptive Spreading Factor techniques dynamically adjust communication parameters to maintain acceptable packet delivery under changing channel conditions. A useful engineering objective for such adaptation may be written as:

$$U = \alpha \cdot PDR - \beta \cdot T_{frame} - \gamma \cdot E, \tag{5}$$

where PDR is packet delivery ratio, T_{frame} is airtime, E is energy cost, and α, β, γ are task-dependent coefficients. This equation reflects the real trade-off between delivery, delay, and endurance [14].

Changing channels or hopping across frequencies can reduce the effectiveness of narrowband interference and attacks based on traffic predictability. Such methods are especially important when the attacker exploits static behavior, although they also increase implementation complexity and energy overhead [17].

Mobile UAV relays can bypass local interference or geographic obstacles by physically changing the communication geometry. Such flexibility is valuable in emergency operations and rapidly changing environments, though limited flight endurance remains a major constraint [13].

4.2 Methods for improving cyber resilience: LoRaWAN 1.1 migration, secure hardware, IDS, geofencing

Cyber resilience differs from basic protection because it includes resistance, detection, response, and recovery [5, 6]. For aviation LoRaWAN systems, this broader perspective is essential because complete prevention is unrealistic in open wireless environments. Protocol migration is one of the most justified baseline measures. LoRaWAN 1.1 improves key handling and session logic, thereby reducing several vulnerabilities associated with older deployments. However, migration should be seen as a starting point rather than a complete solution [12, 20].

The use of Physical Unclonable Functions, secure elements, or TPM-like storage can significantly improve resistance to cloning and key extraction. This is particularly important in aviation contexts where physical access to devices cannot always be prevented [19]. The analytics layer is instantiated as an explainable rule-based IDS to enable reproducible validation of the integrated framework. It uses PDR, the deviation from a pre-attack PDR reference profile, and mean SIR over a 60-s monitoring window. A future ML-based extension can use the same measurements together with RSSI, spreading-factor distribution, airtime, channel occupancy, gateway reception count, packet inter-arrival time, and join-request frequency. With labelled traces, these features can support supervised models such as Random Forest or gradient-boosted trees; with limited labels, they can support unsupervised anomaly detection, for example Isolation Forest [1, 6]. Geofencing is useful for checking whether a device behaves within expected spatial or operational limits. In aviation, this mechanism can be extended from simple location boundaries to mission-aware trust contexts, where unusual spatial behavior triggers stricter verification or isolation.

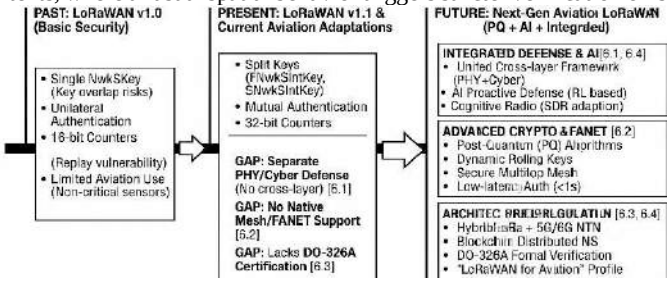


Figure 3. Evolution of LoRaWAN Security: Past (1.0), Present (1.1), Future ($PQ + AI$)

For comparative evaluation, a resilience-oriented score can be written as:

$$R_S = w_1 C + w_2 I + w_3 A + w_4 D \quad (6)$$

where C, I, A, D: C (Confidentiality), I (Integrity), A (Availability), D (Detectability): A theoretical tool to compare and to set priorities for different design decisions during the development of a wireless sensor network given a certain mission profile [5, 6].

Table 2

Main methods for improving cyber resilience

Method	Main objective	Strength	Limitation
LoRaWAN 1.1 migration	Protocol hardening	Better replay and join protection	Does not stop jamming
Secure element / PUF	Key protection	Better capture resistance	Extra hardware cost
ML-based IDS	Attack detection	Finds traffic anomalies	Depends on datasets and tuning
Geofencing	Context validation	Adds mission awareness	Can be bypassed if used alone
Secure rejoin / key rotation	Recovery	Restores trust after suspicion	Increases control complexity

5 Integrated Aviation-Oriented Security Framework

5.1 FANET-specific security challenges and trust management issues

FANET-Specific Security Challenges. The original manuscript already mentioned several FANET-specific security issues different from those typical for terrestrial sensor networks. In this expanded version of the manuscript, we follow this approach and treat the security issues of FANETs as a separate major topic since they fundamentally change the way of communication as well as the way of establishing trust. Dynamic topology is the first challenge for FANETs. The number of possible topologies in a FANET is too high and even changing from time to time in a UAV swarm or in an airborne ad hoc network. As a result, the trust relationships and the sessions of the nodes are changing too and it is difficult to manage and to keep under control such kind of dynamic sensor networks compared to static sensor networks. Relay and routing trust: In standard LoRaWAN end-to-end communication between end nodes is possible. However, for FANETs using LoRaWAN a multi-hop mesh topology is required. Thus, modifications to the standard LoRaWAN protocol or an overlay network have to be implemented. Both approaches introduce additional attack surfaces. These concern intermediate forwarding nodes, routing information as well as the integrity of information that is relayed through the network. In the end, it also has to be investigated which cryptographic concepts in the future could be used in long-endurance flights. As yet, there are only a few first approaches for securing future communications (post-quantum cryptography), which are, however, of only exploratory nature and not yet ready to be used in aviation [13, 20].

5.2 Regulatory and certification requirements for aviation LoRaWAN systems

There are more requirements for higher assurance communication systems in aviation. These also have to fulfill additional documentation, verification and tracing requirements as well as requirements for cyber-assurance of the system in use. LoRaWAN was designed as a communication system for the IoT, thus it is not

suitable for higher assurance applications, like avionics. Therefore an aviation specific implementation of LoRaWAN has to go through formal verification and field validation in order to be considered for use in such environments. This verification and validation process has to check not only the communication protocol but also the used hardware for the trust in the system. Additionally also the trust in the used gateways as well as in the activation process of the sensors and actuators has to be verified. LoRaWAN should not be used as the sole communication bearer for safety-critical flight-control, collision-avoidance, navigation, or time-critical command functions. Its access mechanism, duty-cycle constraints, variable airtime, shared-spectrum interference exposure, and dependence on gateway and backend availability prevent the deterministic latency and bounded communication assurance required by certified avionics systems. Consequently, the appropriate role of LoRaWAN in aviation is limited to non-critical sensing, maintenance telemetry, environmental monitoring, asset tracking, and degraded-mode data collection, provided that operational segregation, fallback paths, and appropriate cybersecurity controls are implemented.

5.3 Integrated cross-layer framework for security and resilience enhancement

In this paper we propose an integrated cross-layer framework for improving security and enhancing resilience of communication systems for air-borne sensor networks of sensing devices. We merge a number of isolated counter-measures against attacks into an unified resilience architecture for use in aviation. The framework consists of a physical resilience layer for radio-adaptive air-borne networks with multiple gateways, a protocol security layer with cryptographically secured activation and session management, a platform trust layer for secure air-borne hardware and post-capture resistance, an analytics layer with an Intrusion Detection System (IDS) for detection of and classification of anomalies, and a recovery layer with mechanisms for secure rejoin of the network, for key-rotation, for fallback to alternative communication systems, and for continuous operation of the mission in degraded mode.

The physical resilience layer of an integrated cross-layer framework for aviation LoRaWAN systems consists of radio components, i.e., airborne devices, and gateway components, i.e., gateways:

1.Platform Security Layer: In order to guarantee secure communication between aircraft and gateways within the aircraft's LoRaWAN network, the Protocol 2.Security Layer enables secure activation of devices as well as protects against replay attacks by managing sessions;

3.Platform trust layer, responsible for secure hardware and post-capture resistance;

4.Analytics layer, for anomaly detection and attack classification;

5.Recovery layer: Secure rejoin of an aircraft, a node or a service, as well as key reversion, fallback to alternative communication as well as continued safe aircraft operation in a degraded mode of operation [6, 12, 19].

5.4 Control logic, recovery mechanisms, and optimization objective

This system operates under a monitoring-assessment-adaptation-recovery control loop. In the moni-toring phase the system could monitor a set of signal parameters

(e.g. the Received Signal Strength Indicator (RSSI) or packet loss) as well as several endpoint parameters (e.g. the number of active gateways per endpoint, timing information, or the complete state of all endpoints). The system could also monitor the details of the join procedure for all endpoints. In the assessment phase the system could make an estimate for the root cause for possible system degradation between congestion, fading, active jamming, packet replay, abused/tampered LoRaWAN infrastructure or endpoint compromise. In the adaptation phase the system communicates with possible system components that could be modified (e.g. modified activation of a backup path and/or isolation of holes in the network and possibly compromised nodes, increased diversity of communication paths between all pairs of endpoints). In the recovery phase the system performs a secure rejoin of the isolated device, it rotates all session keys and possibly switches over to a fallback communication method or even to a reduced function mission mode until all problems have been solved [6, 12, 15].

The framework above will have a general optimization objective as follows:

$$\max J = \lambda_1 A + \lambda_2 I + \lambda_3 PDR - \lambda_4 L - \lambda_5 E \tag{7}$$

subject to mission constraints:

$$Risk \le Risk_{\max} \tag{8}$$

where A is availability, I integrity, PDR packet delivery ratio, L latency, and E energy cost [6].

Table 3

Mapping of threats to integrated mitigation measures

Threat	Main mitigation	Supporting mitigation	Framework layer
Selective/reactive jamming	Adaptive SF, hopping	Multi-gateway, hybrid backup	Physical resilience
Replay	LoRaWAN 1.1, secure session logic	IDS, secure rejoin	Protocol security
Rogue gateway	Gateway trust validation	IDS, backend segmentation	Protocol + analytics
Key extraction	Secure element / PUF	Key rotation	Platform trust
Battery depletion	Join control, anomaly detection	Duty-cycle-aware policies	Analytics + recovery

5.5 Simulation-Based Validation of the Proposed Framework

To complement the analytical framework proposed in this study, a discrete-event Monte Carlo simulation was implemented in MATLAB R2022a. The purpose of the simulation was not to reproduce the complete LoRaWAN protocol stack or to claim certification-level evidence, but to evaluate the relative resilience benefit of the proposed cross-layer architecture for airport-support telemetry. This scope is consistent with the role of LoRaWAN as a low-rate sensing and degraded-mode communication technology rather than as a standalone bearer for safety-critical avionics functions [6, 10, 12]. The simulated network represented an airport-support sensing area of 4 km × 3 km containing 30 end devices. Devices transmitted 24-byte telemetry packets every 60 s during a 1800-s observation interval. The radio

configuration was based on a simplified EU868-like three-channel abstraction with a 125 kHz bandwidth and a transmit power of 14 dBm. A reactive jammer was activated from 600 s to 1200 s on the primary channel. The simulation used 50 Monte Carlo runs for each configuration in order to account for random device locations, path-loss variation, packet collisions, and channel conditions. Two configurations were compared. The baseline configuration used one gateway, a fixed spread-ing factor of SF9, and a static primary channel without attack detection or recovery. The proposed framework used three spatially distributed gateways, adaptive spreading-factor selection, a rule-based anomaly detector, and channel switching after attack detection. The detector used packet delivery ratio degradation and the average SIR as input features. An attack alarm was triggered when the observed PDR and SIR crossed predefined thresholds or when PDR declined by more than 10 percentage points relative to the pre-attack reference profile. After detection, the recovery policy redirected traffic to one of the non-jammed channels. The evaluation considered packet delivery ratio (PDR), packet loss ratio (PLR), mean end-to-end latency, mean transmission energy, the Jamming Resilience Index (JRI), attack detection rate, false-positive rate, detection delay, and recovery time. The JRI was calculated as:

$$JRI = \frac{PDR_{jammed}}{PDR_{Normal}} \tag{9}$$

Table 4

Simulation parameters

Parameter	Value
Evaluation method	Discrete-event Monte Carlo simulation
Number of Monte Carlo runs	50
Simulated area	4 km × 3 km airport-support area
Number of end devices	30
Simulation duration	1800 s
Telemetry transmission period	60 s
Payload size	24 bytes
Channel abstraction	Three EU868-like channels (868.1, 868.3, 868.5 MHz)
Bandwidth	125 kHz
Coding rate parameter	CR = 1
Transmit power	14 dBm
Baseline gateways	1
Proposed framework gateways	3
Baseline spreading factor	Fixed SF9
Proposed spreading factor	Adaptive SF7, SF9, or SF11
Jamming type	Reactive channel-targeted jamming
Jamming interval	600–1200 s
Jammed channel	Primary channel (868.1 MHz)
Jammer power (rel. to signal)	+10 dB on the jammed channel
Adjacent-channel leakage	-18 dB (relative to useful signal)
IDS observation window	60 s
IDS thresholds	PDR: 0.85, PDR-drop: 0.10, SIR: 0 dB
Recovery policy	Channel switching (Ch 2 or 3), adaptive SF, gateway diversity
Recovery PDR target	0.80

A JRI close to one indicates that the network preserves most of its normal-operation delivery performance under jamming. The simulation parameters are summarized in table below. The results in Table 5 and Figure 4 show that the proposed framework substantially improves communication availability. Under normal conditions, PDR increased from 75.25% in the baseline configuration to 96.64% in the proposed configuration. During reactive jamming, the baseline PDR decreased to 57.45%, whereas the proposed framework maintained a PDR of 94.54%. Therefore, the proposed configuration achieved an absolute PDR gain of 37.09 percentage points and a relative improvement of 64.51% under jamming. The corresponding JRI increased from 0.7639 in the baseline configuration to 0.9783 in the proposed framework, as shown in Figure 5.

Table 5

Results and performance comparison

Metric	Baseline	Proposed	Change
PDR (normal operation), %	75.25	96.64	+28.42%
PDR (reactive jamming), %	57.45	94.54	+64.51%
PLR (reactive jamming), %	42.55	5.46	-87.17%
Jamming Resilience Index (JRI)	0.7639	0.9783	+28.68%
Mean end-to-end latency, ms	248.82	377.39	+51.67%
Mean transmission energy, mJ	5.17	8.30	+60.54%

This result indicates that the cross-layer design preserved approximately 97.8% of its normal-operation PDR during the attack. The improvement is associated with the combined effect of gateway diversity, adaptive spreading-factor selection, and channel switching after anomaly detection. These mechanisms are consistent with the physical-resilience and recovery layers of the proposed framework [6, 14, 15, 16].

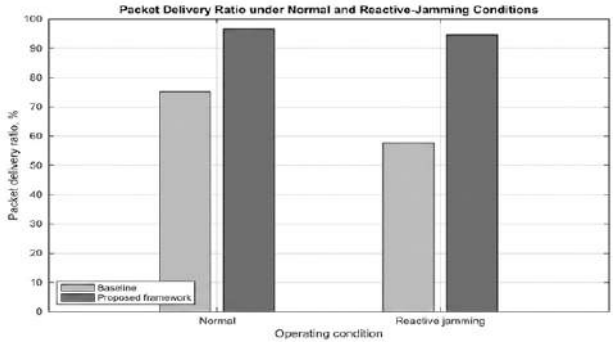


Figure 4. Packet delivery ratio under normal operation and reactive-jamming conditions.

The rule-based IDS detected the jamming event in all simulation runs. Its event-level detection rate was 100%, while the false-positive rate was 0.7%. The mean

detection delay was 76.8 s, which is consistent with the 60-s observation window, and the mean recovery time after detection was 60 s. Figure 7 summarizes these IDS and recovery results. The findings demonstrate that the framework can support a monitoring–assessment–adaptation–recovery cycle for non-critical airport sensing and telemetry applications. The resilience improvement was accompanied by an expected efficiency trade-off. The mean end-to-end latency increased from 248.82 ms to 377.39 ms, while mean transmission energy increased from 5.17 mJ to 8.30 mJ. This increase is explained by adaptive selection of higher spreading factors for adverse links and by additional reception opportunities in the multi-gateway configuration. Hence, the proposed framework improves availability and jamming resilience at the cost of latency and energy, which confirms that aviation-oriented LoRaWAN design should be treated as a constrained multi-objective optimization problem.

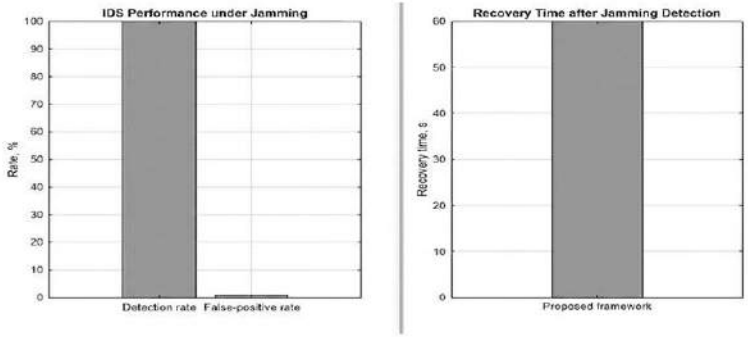


Figure 5. Jamming Resilience Index for the baseline and proposed framework configurations.

The presented results should be interpreted as simulation-based evidence for airport-support telemetry, perimeter monitoring, maintenance diagnostics, and degraded-mode data collection. They do not establish compliance with certification requirements and do not justify the use of LoRaWAN as the sole communication technology for safety-critical flight-control or avionics functions. Field experiments, hardware-in-the-loop validation, realistic RF measurements, and further analysis of protocol-layer attacks remain necessary before operational deployment.

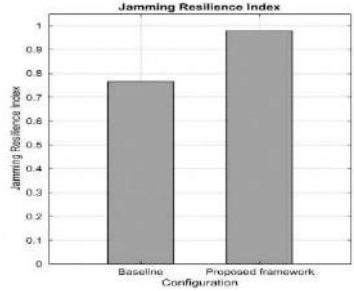


Figure 6. IDS and recovery performance of the proposed framework under reactive jamming

6 Future Research and Conclusions

6.1 Open research problems in aviation LoRaWAN security

There are many issues to be addressed for the application of LoRaWAN in the aviation area, as has been described in recent research. First of all, an integrated cross-layer model has to be developed which not only supports radio adaptation but also supports attack detection, trust management and continuous mission execution when under attack. There is no single formally analyzable model that fulfills all of these requirements. IDS realism: There is a severe lack of suitable data sets for the training and evaluation of IDS detection models. Suitable data sets must comprise a wide variety of different scenarios, including different types of mobility, various kinds of single and combined interference as well as coordinated attacks on the network as well as normal operation with all possible types of variability. The accuracy that has been reported so far is not guaranteed to be sufficient for the actual application in real FANETs [6]. FANETs: Design of FANET-native protocol adaptations to support secure split/merge of relays, reduced capability relays, very fast re-auth. Small aircraft (ULM/L). Aviation-specific standards and assurance profiles for FANETs using LoRaWAN. The issue of secure key usage over long time spans corresponds to the long time of missions and even longer to the certification time of those keys also after transition to post-quantum cryptography [13, 19, 20]. A priority for future work is the replacement or augmentation of the rule-based IDS with a data-driven model trained on representative airport-support LoRaWAN traces. Such an evaluation should compare detection accuracy, precision, recall, false-positive rate, inference delay, and computational overhead for supervised and unsupervised models under jamming, congestion, replay, rogue-gateway, and battery-depletion scenarios.

6.2 Final conclusions and practical implications for aviation deployment

The simulation-based validation performed in this study provides quantitative support for the proposed cross-layer framework. In the modeled airport-support telemetry scenario, the proposed configuration increased PDR under reactive jamming from 57.45% to 94.54% and increased the Jamming Resilience Index from 0.7639 to 0.9783. The rule-based IDS detected the jamming event in all Monte Carlo runs with a mean detection delay of 76.8 s and a 0.7% false-positive rate, while the recovery policy restored the target PDR within 60 s after detection. These results indicate that combining gateway diversity, adaptive radio parameters, attack detection, and channel switching can substantially improve LoRaWAN availability under targeted interference. The article states that long-range low power communication system like LoRaWAN 1.1 is very useful for distributed infrastructure with high maintenance cost, for very sparse deployed stations and for autonomous systems. Therefore, we could concludes that LoRaWAN 1.1 is very promising for sensing and telemetry applications, for communication between a swarm of UAVs and for airport monitoring applications. In addition, the author states that LoRaWAN 1.1 is very promising for a degraded mode of communication in case of failure of primary communication system.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] L. Paredes, H. Kaushal, T. V. Pasca, LoRa Technology in Flying Ad Hoc Networks: A Survey of Challenges and Open Issues, Sensors 23 (5) (2023) 2403. doi: 10.3390/s23052403.

[2] A. Nissim, LoRaWAN in Physical Security & Aviation: A Quiet Revolution in Awareness, LinkedIn, Apr. 19, 2025. [Online]. Available: https://www.linkedin.com/pulse/ lorawan-physical-security-aviation-quiet-revolution-awareness-nissim-bvyue/.

[3] T. K. Bhatia, S. Gilhotra, S. S. Bhandari, R. Suden, Flying Ad-Hoc Networks (FANETs): A Review, EAI Endorsed Transactions on Energy Web 11 (2024). doi: 10.4108/ew.5489.

[4] R. Ronen, B. Ben-Moshe, Cyberattack on Flight Safety: Detection and Mitigation Using LoRa, Sensors 21 (13) (2021) 4610. doi: 10.3390/s21134610.

[5] F. Hessel, L. Almon, M. Hollick, LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation, ACM Transactions on Sensor Networks 18 (4) (2023) 1-55. doi: 10.1145/3561973.

[6] M. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang, LoRaWAN security survey: Issues, threats and possible mitigation techniques, Internet of Things 14 (2021) 100303. doi: 10.1016/j.iot.2021.100303.

[7] M. Butun, N. Pereira, M. Gidlund, Security Vulnerabilities in LoRaWAN, in: Proceedings of the 3rd ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects, ACM, 2018, pp. 1-6. doi: 10.1145/3213299.3213304.

[8] Z. Moha, Y. Chen, I.-R. Cho, A Malicious Behavior Awareness and Defense on LoRa IoT, Sensors 19 (23) (2019) 5122. doi: 10.3390/s19235122.

[9] J. Haxhibeqiri, E. De Poorter, I. Moerman, J. Hoebeke, A Survey of LoRaWAN for IoT: From Technology to Application, Sensors 18 (11) (2018) 1-38. doi: 10.3390/s18113995.

[10] A. Povalac, A. Kral, J. Arthaber, O. Kolar, M. Novak, Exploring LoRaWAN Traffic: In-Depth Analysis of IoT Network Communications, Sensors 23 (17) (2023) 7333. Online publication date: 22-Aug-2023. doi: 10.3390/s23177333.

[11] A. Mehic, M. A. Alrshaid, M. A. AlSarawi, Analysis of LoRaWAN 1.0 and 1.1 Protocols Security Mechanisms, Sensors 22 (10) (2022) 3690. doi: 10.3390/s22103690.

[12] V. Kalokidou, M. Nair, M. A. Beach, LoRaWAN Performance Evaluation and Resilience under Jamming Attacks, in: 2022 Sensor Signal Processing for Defence Conference (SSPD), IEEE, 2022, pp. 1-5. doi: 10.1109/SSPD56389. 2022.9896225.

[13]H. Ruotsalainen, Y. Shen, M. A. AlGhadi, A. S. Alghamdi, LoRaWAN Physical Layer-Based Attacks and Countermeasures, A Review, Sensors 22 (8) (2022) 2770. doi: 10.3390/s22082770.

[14] M. Saifullah, McMullen, Impact of Reactive Jamming Attacks on LoRaWAN: A Theoretical Assessment and Experimental Validation, in: Proceedings of the 23rd International Confer-ence on Distributed Computing and Networking (ICDCN 2024), ACM, 2024, pp. 1-10. doi: 10.1145/3538969.3543805.

[15] H. Ningning, X. Xianjin, Z. Yuanqing, Jamming of LoRa PHY and Countermeasure, in: IEEE INFOCOM 2021, IEEE, 2021, pp. 1-10. doi: 10.1109/INFOCOM42981. 2021.9488774.

[16] N. Prasad, P. Lynggaard, LoRaWan Sensitivity Analysis and Prevention Strategies Against Wireless DoS Attacks, Wireless Personal Communications 124 (4) (2022) 2343-2360. doi: 10.1007/s11277-022-09884-8.

[17] A. Shamsoshoara, A. Korenda, F. Afghah, S. Zeadally, A survey on physical unclonable function (PUF)-based security solutions for Internet of Things, Computer Networks 180 (2020) 107593. doi: 10.1016/j.comnet.2020.107593.

[18] M. Mehic, I. Begovic, S. Omanovic, N. Suljanovic, LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios, ETT 33 (10) (2021) 1-24. doi: 10.1002/ett.4452.

[19] S. You, J. Kwon, An Enhanced LoRaWAN Security Protocol for Privacy Preservation in IoT with a Case Study on a Smart Factory-Enabled Parking System, Sensors 18 (6) (2018) 1888. doi: 10.3390/s18061888.

[20] Trend Micro Research, Low-Powered but High-Risk: Evaluating Possible Attacks on LoRaWAN De-vices, Trend Micro, Jan. 25, 2021. [Online]. Available: https://www.trendmicro.com/en_us/research/ 21/a/Low-Powered-but-High-Risk-Evaluating-Possible-Attacks-on-LoRaWAN-Devices.html.

LORAWAN В АВІАЦІЇ: КОМПЛЕКСНИЙ АНАЛІЗ КІБЕРЗАГРОЗ ТА СТРАТЕГІЙ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ

Тертус Ю., Козловська Д., Dr.Sci., Козловський В., Котик Б.
Національний університет "Київський Авіаційний інститут", Україна

Анотація: *Швидкий розвиток авіаційних кіберфізичних систем, зокрема БПЛА та «розумних» аеропортів, потребує далекобійних та енергоефективних комунікацій. Технологія LoRaWAN є однією з найперспективніших для таких завдань, проте суворі вимоги авіації до безперервності зв'язку, затримок та кіберстійкості роблять її впровадження без адаптації небезпечним. У цій статті систематизовано властивості LoRa/LoRaWAN, проаналізовано сценарії розгортання, формалізовано багаторівневу модель загроз і запропоновано інтегровану архітектуру, адаптовану до потреб авіації. Ефективність рішення підтверджено моделюванням методом Монте-Карло в MATLAB, яке імітує роботу телеметрії аеропорту в умовах нормальної експлуатації та реактивного заглушення. Результати демонструють покращену доставку пакетів та швидке відновлення після атак, створюючи основу для проектування надійних авіаційних мереж LoRaWAN.*

Ключові слова: *LoRaWAN, кібербезпека, стійкість до перешкод, штучний інтелект, обробка даних, машинне навчання*

УДК 004.934:004.85
DOI

ОСОБЛИВОСТІ ДОНАВЧАННЯ АУДІОМОДАЛЬНИХ ВЕЛИКОМОВНИХ МОДЕЛЕЙ: OMNIVOICE, FISHAUDIO2 (FISHSPEECH S2) ТА QWEN3 AUDIO

Dr.Sci., Пелешко Д.[1][0000-0003-3412-1639], Пелешко С.-Д.[2][0009-0002-7474-0725], Dr.Sci., Винокурова О.[3][0000-0002-9421-8566], Ph.D., Пелешко М.[4][0000-0002-9315-1590]
[1,3]Львівський національний університет ім. І. Франка
[2]Український католицький університет
[4]Львівський державний університет безпеки життєдіяльності
EMAIL: [1] dpeleshko@gmail.com, [2]severyn,peleshko@gmail.com, [3]vynokurova@gmail.com, [4]marta.peleshko@gmail.com

Анотація. *Створення якісних українськомовних систем синтезу мовлення ускладнюється низькоресурсністю української мови та обмеженістю доступного апаратного забезпечення. Сучасні аудіомодальні великомовні моделі демонструють високу якість zero-shot синтезу, проте можливості їх донавчання для української мови на графічних процесорах середнього класу залишаються недостатньо дослідженими.* ***Мета.*** *Провести порівняльне дослідження моделей OmniVoice, FishAudio2 (Fish Speech S2) та Qwen3-TTS для визначення можливостей їх донавчання для української мови на кластері з чотирьох графічних процесорів NVIDIA Tesla T4.* ***Методи.*** *Проаналізовано архітектурні парадигми моделей (неавторегресійну дифузійну, подвійну авторегресійну та Thinker-Talker із сумішшю експертів), їх лінгвістичне охоплення, засоби керування тривалістю, темпом та емоціями мовлення, продуктивність інференсу, вимоги до підготовки наборів даних, а також апаратні обмеження архітектури Turing.* ***Результати.*** *Встановлено, що OmniVoice поєднує базову підтримку української мови, точне керування тривалістю та швидкістю мовлення і найвищу швидкодію (коефіцієнт реального часу, RTF, 0.025), а обмеження ядра flex_attention щодо розподіленої пам'яті T4 долається переходом на механізм уваги SDPA (Scaled Dot-Product Attention). Qwen3-TTS забезпечує найкраще керування емоціями через системні промпти, але потребує значно більшого набору даних для навчання української фонетики та виправлення помилок у навчальних скриптах. FishAudio2 генерує найвиразніше мовлення з частотою дискретизації 44.1 кГц, проте розмір 4.4 млрд параметрів і відсутність керування швидкістю у відкритому коді роблять її донавчання на T4 недоцільним.* ***Висновки.*** *Для донавчання моделі синтезу української мови на кластері Tesla T4 рекомендовано OmniVoice; Qwen3-TTS є альтернативою для діалогових агентів за умови формування розширеного українського набору даних.*

Ключові слова: *синтез мовлення; аудіомодальні великомовні моделі; донавчання; українська мова; OmniVoice; Fish Speech; Qwen3-TTS; NVIDIA Tesla T4; клонування голосу; керування тривалістю мовлення.*

1. Вступ

Аналіз зосереджено на критичних параметрах навчання та практичного використання цих моделей у промисловій експлуатації. До параметрів використання належать можливості детермінованого керування тривалістю звукової доріжки, здатність моделі до відтворення емоцій, клонування голосу, а також загальна швидкість інференсу. До параметрів навчання належать оцінка можливості донавчання на наявному апаратному забезпеченні середнього класу

(NVIDIA Tesla T4), аналіз архітектурних парадигм кожної моделі, а також процеси підготовки наборів даних та специфіка роботи з кириличною фонетикою. Мета – провести порівняльне дослідження моделей OmniVoice, FishAudio2 (Fish Speech S2) та Qwen3 Audio для визначення можливостей донавчання моделей української мови на кластері NVIDIA Turing (Tesla T4, 4 графічні процесори по 16 ГБ VRAM (Video Random Access Memory, відеопам'ять)).

2. Аналіз останніх досліджень і публікацій

Сучасні системи синтезу мовлення (text-to-speech, TTS) переважно ґрунтуються на архітектурі трансформера [1], яка замінила рекурентні та згорткові мережі в задачах перетворення послідовностей завдяки механізму уваги та високому ступеню паралелізації навчання. Раннє покоління нейромережевих TTS-систем мало двоетапну будову: акустична модель генерувала мел-спектрограму, а окремий вокодер перетворював її на хвильову форму. Показовим прикладом є вокодер HiFi-GAN [2], побудований на генеративних змагальних мережах (generative adversarial networks, GAN), який завдяки моделюванню періодичних складових сигналу забезпечив якість, близьку до людської, за швидкості генерації, що значно перевищує реальний час. Модель VITS (Variational Inference with adversarial learning for end-to-end Text-to-Speech) [3] об'єднала обидва етапи в єдину end-to-end архітектуру на основі умовного варіаційного автокодувальника з adversarial-навчанням і стохастичним предиктором тривалостей. Разом з тим такі системи потребували значних обсягів даних від конкретного диктора та не підтримували клонування голосу без донавчання. Якісно новий етап пов'язаний з появою нейронних аудіокодеків, які перетворюють неперервний звуковий сигнал на послідовність дискретних токенів. SoundStream [4] запропонував повністю згортковий кодек із залишковим векторним квантуванням (residual vector quantization, RVQ), здатний працювати в діапазоні бітрейтів від 3 до 18 кбіт/с, а EnCodec [5] розвинув цей підхід для потокового кодування аудіо з частотою дискретизації 24 і 48 кГц. Саме багаторівневі словники RVQ (multi-codebook) стали базовим представленням звуку для більшості аудіомоделей, що розглядаються в цій статті. Спираючись на такі кодеки, автори VALL-E [6] уперше сформулювали задачу TTS як умовне мовне моделювання кодекових токенів і продемонстрували синтез голосу невідомого диктора за 3-секундним фрагментом референсного аудіо (zero-shot TTS). Авторегресійна (AR) парадигма отримала подальший розвиток у сімействі Seed-TTS [7], яке досягло якості синтезу, практично невідрізнюваної від людського мовлення, та в системі CosyVoice [8], де запропоновано супервізовані семантичні токени, отримані з багатомовної моделі розпізнавання мовлення, у поєднанні з conditional flow matching для реконструкції спектрограми. Водночас AR-моделям притаманне принципове обмеження: оскільки генерація відбувається токен за токеном, точне керування тривалістю синтезованого мовлення є складним. У роботі IndexTTS2 [9] запропоновано перший для великих AR-моделей механізм явного задання кількості генерованих токенів, а також розділення тембру та емоційної складової, що є критичним для задач автоматичного дубляжу.

Альтернативу становлять неавторегресійні (NAR) підходи. E2 TTS [10] показала, що мел-спектрограму можна генерувати методом flow matching з текстової послідовності, доповненої токенами-заповнювачами, без моделі тривалостей і перетворення графем у фонеми (grapheme-to-phoneme, G2P). F5-TTS [11] удосконалила цю схему, використавши Diffusion Transformer з блоками ConvNeXt V2 та стратегію семплювання Sway Sampling, і досягла коефіцієнта реального часу (real-time factor, RTF) 0,15. MaskGCT (Masked Generative Codec Transformer) [12] перенесла в синтез мовлення парадигму маскованого генеративного моделювання, запропоновану для зображень у MaskGIT (Masked Generative Image Transformer) [13], за якої всі токени генеруються паралельно з поступовим ітеративним розмаскуванням; важливою властивістю такого підходу є можливість задавати загальну тривалість згенерованого мовлення. OmniVoice [14] розвиває цей напрям: модель безпосередньо відображає текст у багатокодбукові акустичні токени, використовує стратегію повнокодбукового випадкового маскування та ініціалізацію вагами попередньо навченої великої мовної моделі (LLM), що дозволило масштабувати підтримку до понад 600 мов на базі 581 тис. годин відкритих даних. Окремий напрям становлять моделі, що будують синтез мовлення на основі LLM із подвійною авторегресією. Fish-Speech [15] запропонувала послідовну «повільну-швидку» архітектуру Dual-AR у поєднанні з груповaним скалярним квантуванням, що дозволило використовувати LLM для вилучення лінгвістичних ознак без попереднього G2P-перетворення. Fish Audio S2 [16] масштабувала цей підхід, доповнивши його багатоетапним навчанням, вирівнюванням методами навчання з підкріпленням та керуванням просодією й емоціями за допомогою текстових інструкцій. Сімейство моделей Qwen реалізує іншу концепцію – архітектуру Thinker-Talker, уперше описану в Qwen2.5-Omni [17], де модуль Thinker генерує текст і високорівневі представлення, а двотрековий авторегресійний модуль Talker – потокові аудіотокени. У Qwen3-Omni [18] обидва модулі переведено на архітектуру суміші експертів (Mixture-of-Experts, MoE) [19], а блокову дифузію замінено легкою каузальною згортковою мережею (convolutional network, ConvNet), що забезпечило теоретичну затримку першого пакета 234 мс у режимі холодного старту. Спеціалізована серія Qwen3-TTS [20] використовує двотрекову мовну модель і токенізатор з частотою 12,5 Гц та 16-рівневим словником, досягаючи затримки першого пакета 97 мс; водночас її навчальний корпус охоплює лише 10 мов, серед яких українська відсутня. Для якісного синтезу українського мовлення визначальною є мовна репрезентативність навчальних даних. Відкриті корпуси Common Voice [21] та FLEURS (Few-shot Learning Evaluation of Universal Representations of Speech) [22] містять українські записи, проте їхній обсяг на порядки менший порівняно з англійською чи китайською мовами, що відносить українську до низькоресурсних мов. Проєкт Massively Multilingual Speech [23] продемонстрував можливість масштабування мовленнєвих технологій на понад тисячу мов за рахунок самокерованого навчання, а модель Whisper [24] – що слабко-супервізоване навчання на 680 тис. годин забезпечує робастне

багатомовне розпізнавання мовлення; саме Whisper широко застосовується в сучасних TTS-системах для автоматичної транскрипції референсного аудіо.

Практичне донавчання моделей із сотнями мільйонів і мільярдами параметрів на обмеженому апаратному забезпеченні спирається на низку технік ефективного навчання. Метод LoRA (Low-Rank Adaptation) [25] дозволяє заморозити базові ваги моделі та навчати лише низькорангові матриці адаптації, що на порядки зменшує кількість параметрів, які оновлюються. Оптимізатор ZeRO (Zero Redundancy Optimizer) [26] усуває дублювання станів оптимізатора, градієнтів і параметрів між процесами за паралелізму даних. Навчання зі змішаною точністю [27] майже вдвічі знижує вимоги до пам'яті, однак у 16-бітному форматі з рухомою комою половинної точності (float16) потребує масштабування функції втрат для запобігання втраті малих значень градієнтів. Ефективність механізму уваги значною мірою визначається реалізацією обчислювальних ядер: FlashAttention [28] застосовує тайлінг для зменшення кількості звернень до глобальної пам'яті графічного процесора (graphics processing unit, GPU), а FlexAttention [29] генерує оптимізовані ядра для довільних варіантів уваги за допомогою компілятора, при цьому конфігурація блоків таких ядер залежить від обсягу розподіленої (shared) пам'яті потокового мультипроцесора. Для акустичного моделювання також застосовують спеціалізовані енкодери на кшталт Zipformer [30], що використовує U-Net-подібну структуру з різними частотами кадрів.

Аналіз публікацій засвідчує, що більшість робіт оцінює моделі на високопродуктивних прискорювачах та для високоресурсних мов. Натомість систематичного порівняння можливостей донавчання OmniVoice, Fish Audio S2 та Qwen3-TTS для української мови на апаратному забезпеченні середнього класу, зокрема на графічних процесорах архітектури Turing без апаратної підтримки формату bfloat16 (Brain Floating Point, 16-бітний формат з плаваючою комою з розширеним діапазоном порядку), у відкритих джерелах не виявлено, що й зумовлює актуальність цього дослідження.

3. Архітектурні особливості моделей

3.1 OmniVoice

OmniVoice (розробка команди Xiaomi/Kaldi) реалізує принципово відмінний від інших розглянутих моделей підхід до синтезу мовлення. Це доволі масштабна багатомовна модель, архітектуру якої визначають як дифузійну мовну модель дискретного неавторегресійного (NAR) типу. Для розуміння переваг неавторегресійного підходу доцільно розглянути класичний авторегресійний (AR) підхід. AR-моделі генерують аудіотокени послідовно, крок за кроком. Наприклад, для синтезу 10 с аудіо модель має виконати сотні або тисячі послідовних ітерацій. Це, по-перше, суттєво збільшує час генерації, а по-друге, спричиняє накопичення помилок: похибка, допущена на початку послідовності, поширюється на всі наступні кроки. Неавторегресійна дифузійна парадигма працює принципово інакше: замість послідовного передбачення «зліва направо» модель бере матрицю випадкового шуму (або маскованих токенів) потрібної довжини й оновлює всі токени одночасно за кілька кроків знешумлення. На кожному кроці дифузії впевненість моделі в

передбаченнях зростає, і випадкові значення поступово замінюються чіткими акустичними токенами (ітеративне розмаскування, iterative unmasking).

Основною проблемою традиційних NAR-моделей є так зване «вузьке місце» продуктивності, зумовлене складними дворівневими конвеєрами: текст спочатку перетворюється на семантичні токени, а потім – на акустичні токени, тобто цілочисельні індекси в багаторівневому словнику (multi-codebook), з яких відновлюються короткі фрагменти аудіосигналу. Розглянемо принцип роботи багаторівневого словника. Якщо вихідний звуковий сигнал позначити як X, а його наближення першим рівнем – як C1, то другий рівень кодує різницю X – C1, третій – залишок X – C1 – C2 і т. д. В OmniVoice використовуються чотири рівні словників: перший (базовий) кодує фонетику, другий – тембр та інтонацію, третій і четвертий – акустичні характеристики та дрібні деталі. У результаті кожні 20 мс аудіо описуються не одним токеном, а матрицею токенів. Саме цю багатокодову матрицю модель навчається відновлювати та генерувати в процесі дифузії. Принциповою особливістю OmniVoice є пряме відображення тексту в багатокодові акустичні токени без проміжних стадій. У неавторегресійних дифузійних моделях для аудіо (і тексту) роль шуму виконує маскування. Під час навчання (прямий процес) модель отримує аудіопослідовність, розбиту на токени, і крок за кроком випадково замінює їх на спеціальний токен [MASK]. На завершальному етапі дифузії замаскованими є 100 % токенів, що є аналогом повного білого шуму в дифузійних моделях зображень. Під час генерації (зворотний процес, знешумлення) модель починає з послідовності, яка складається виключно з токенів [MASK], і її завдання полягає в тому, щоб за кілька паралельних ітерацій передбачити, які акустичні токени мають стояти на місці масок, спираючись на вхідний текст. Автори OmniVoice виділяють дві ключові інновації. Перша – стратегія випадкового маскування всього кодового словника (full-codebook random masking) під час навчання, яка змушує модель вивчати взаємозв'язки між акустичними одиницями паралельно, а не послідовно. Друга – ініціалізація моделі вагами попередньо навченої текстової великої мовної моделі (LLM). За твердженням розробників, знання, набуті LLM під час попереднього навчання, ефективно переносяться на двонаправлену (bidirectional) архітектуру OmniVoice. Інакше кажучи, параметри текстової моделі, навченої на великих корпусах і здатної до глибокого розуміння природної мови, використовуються як початкова точка навчання. Слід зазначити, що класичні LLM навчаються з каузальною маскою, тобто враховують лише попередній контекст. Натомість OmniVoice як неавторегресійна дифузійна модель є двонаправленою: вона генерує всі звукові токени одночасно й паралельно, тому потребує доступу до всього тексту відразу (як до початку, так і до кінця речення). Для цього автори застосовують вилучення каузальної маски, що фактично перетворює LLM на двонаправлену модель; детальний аналіз цього механізму виходить за межі цього дослідження. Перенесення знань дозволяє OmniVoice «перепрофілювати величезну лінгвістичну ємність LLM як потужний апріорний базис для покращення розбірливості та природності згенерованого мовлення». На практиці це означає, що для природного озвучення речення модель має визначати місця пауз, підвищення тону та логічних наголосів. Звичайні TTS-моделі змушені вивчати

ці закономірності з нуля на основі аудіозаписів, що є складною задачею. OmniVoice завдяки знанням LLM уже володіє семантичним уявленням про те, як має звучати речення, і їй залишається лише перетворити це уявлення на акустичні токени. Саме це забезпечує високу природність і розбірливість вимови. Для сучасних LLM 0,6 млрд параметрів – невеликий обсяг (найбільші моделі мають сотні мільярдів параметрів), однак для моделі синтезу мовлення він є значним. Оскільки модель ініціалізовано вагами LLM, їй не потрібно витрачати параметри на вивчення мови з нуля, і всі 0,6 млрд параметрів спрямовано на підвищення якості звуку. Завдяки дифузійній двонаправленій архітектурі модель генерує всі звукові токени паралельно, не очікуючи завершення генерації попередніх фрагментів, що забезпечує майже миттєвий синтез усього аудіо.

3.2 Qwen3-Audio

Сімейство моделей Qwen3-Audio, розроблене командою Alibaba Cloud, функціонує на базі архітектури Thinker-Talker, яка об'єднує процеси сприйняття та генерації в єдиний мультимодальний конвеєр. Архітектура складається з двох ключових трансформерних модулів, побудованих за принципом Mixture-of-Experts (MoE). Thinker обробляє вхідний текст або інструкцію; його завдання полягає у визначенні змісту, контексту та емоційного забарвлення. Цей трансформер не генерує звук, а формує високорівневі представлення. Talker отримує ці представлення й перетворює їх на акустичні токени (аналогічні описаним для OmniVoice). Суміш експертів (MoE) – архітектурний підхід, спрямований на економію обчислювальних ресурсів. Нейромережа Qwen3 складається з великої кількості менших підмереж («експертів»). Під час генерації звуку активується не вся модель, а лише ті її частини, що відповідають за поточне завдання (наприклад, експерт з англійської мови або експерт із синтезу шепоту). Це забезпечує високу швидкодію та знижує вимоги до ресурсів під час запуску.

Модель використовує власний токенізатор Qwen3-TTS-Tokenizer-12Hz, який забезпечує високоефективне акустичне стиснення сигналу за низької частоти кадрів (12 Гц). Це дозволяє повністю зберегти паралінгвістичну інформацію, зокрема тембр, фоновий шум та акустичні властивості приміщення, в якому перебував еталонний диктор. Частота 12 Гц відповідає дуже високому ступеню стиснення: типова частота дискретизації мовленнєвого аудіо становить 24 кГц, і поширені токенізатори стискають його до 50 або 75 токенів на секунду, тоді як токенізатор Qwen3 генерує лише 12 токенів на секунду аудіо. Відповідно, модуль Talker має передбачати значно менше даних, що суттєво пришвидшує його роботу без втрати деталей голосу.

Відмова від DiT (Diffusion Transformer, дифузійний трансформер) на користь легкої ConvNet (у модулі Code2Wav) є ключовою відмінністю Qwen3-Audio від OmniVoice. Модуль Code2Wav є завершальним етапом роботи моделі, на якому акустичні токени перетворюються на звукову хвилю. Дифузійні моделі (DiT), що використовуються в OmniVoice, працюють паралельно й потребують кількох ітерацій знешумлення; вони формують звук лише після повної генерації речення, тому необхідно очікувати завершення синтезу всього аудіо. У Qwen3 дифузію замінено каузальною ConvNet. Термін «каузальна»

означає, що мережа використовує лише попередній контекст (аналогічно каузальній масці, згаданій під час опису OmniVoice). Завдяки цьому щойно Talker генерує перший токен (що відповідає першій 1/12 секунди аудіо), ConvNet одразу перетворює його на звук. Як наслідок, немає потреби очікувати завершення інференсу, і модель починає відтворювати мовлення майже миттєво.

3.3 FishAudio2 та елементи IndexTTS2 архітектури

Основою системи є архітектура, подібна до LLaMA, яка використовується для відображення вхідних текстових послідовностей у проміжні семантичні токени, що надалі перетворюються на акустичні токени.

FishAudio2 є найбільшою серед трьох розглянутих моделей: версія Fish Audio2 має близько 4,4 млрд параметрів, що є значним обсягом для аудіомоделі. Такий розмір дозволяє моделі засвоїти велику кількість особливостей людського мовлення (акцентів, придихань, емоцій) і забезпечує надзвичайно якісний і природний звук. Водночас для її запуску та експлуатації потрібні високопродуктивні й дорогі графічні процесори.

В основі моделі лежить подвійна авторегресія (Dual-AR). Авторегресія (AR) – це спосіб генерації, за якого результат формується поетапно: на кожному кроці модель враховує вже згенероване й на цій основі передбачає наступний елемент. Термін «подвійна» (dual) означає, що генерація відбувається у два послідовні проходи, де один авторегресійний процес слідує за іншим. Саме подвійна авторегресія та подальша генерація аудіо відрізняють FishAudio2 від IndexTTS2. В IndexTTS2 також передбачено два етапи, проте перший із них є авторегресійним, а другий – неавторегресійним (як в OmniVoice). Отже, IndexTTS2 займає проміжне положення між FishAudio2 та OmniVoice. Архітектура моделі подібна до LLaMA (Meta) чи ChatGPT, тобто ґрунтується на трансформері, що складається лише з декодера (decoder-only transformer). Замість створення спеціалізованої аудіомоделі з нуля автори побудували її як мовну модель. Це означає, що аудіо сприймається не як неперервна звукова хвиля, а як послідовність числових кодів. Завдяки цьому модель ефективно враховує контекст тексту, логічні наголоси та навіть емоційні інструкції в дужках (наприклад, [шепіт] або [професійний тон]), обробляючи їх як звичайні слова.

На відміну від OmniVoice, відображення є повним: текст → семантичні токени → акустичні токени:

- Крок 1 (текст → семантичні токени): модель обробляє текст і перетворює його на семантичні токени, які ще не є звуком, а відображають зміст та емоційне забарвлення майбутнього мовлення.
- Крок 2 (семантичні токени → акустичні ознаки): семантичні токени перетворюються на акустичні, тобто на фізичні характеристики звукової хвилі – висоту голосу, тембр, шуми, дихання. На цьому етапі формується кінцевий аудіосигнал.

Слід звернути увагу, що багаторівневий словник (codebook) FishAudio2 складається з 10 рівнів (на відміну від 4 в OmniVoice). Відповідно, кожен кадр описується десятьма словниками: 1-й словник: базова семантика (зміст, вимова,

основна інтонація); 2–10-й словники: залишкові акустичні деталі (тембр, мікроінтонації, гучність, дихання).

Для відображення застосовується семантичне стиснення від 50 до 25 Гц (подібне до OmniVoice, але з іншими параметрами). Тобто модель розбиває аудіо на короткі фрагменти: якщо за замовчуванням формувалося 50 семантичних токенів на кожну секунду звуку (50 Гц), то розробникам вдалося вмістити ту саму інформацію лише у 25 кадрів (25 Гц).

Завдяки цьому довжина послідовності, яку обробляє модель, скорочується вдвічі.

Після відображення запускається Dual-AR. Якби система генерувала всі 10 словників в одну послідовність, її довжина зросла б у 10 разів, що суттєво уповільнило б інференс. Тому архітектуру розділено на два проходи. Slow AR (повільна авторегресія): найбільша частина моделі (4 млрд параметрів), яка виконується вздовж осі часу (кадр за кадром) і передбачає лише перший словник. Fast AR (швидка авторегресія): легкий модуль на 400 млн параметрів. Отримавши базовий токен від Slow AR, Fast AR рухається вздовж осі глибини й для того самого кадру швидко генерує решту 9 акустичних словників.

Для отримання звуку акустичні токени декодуються вокодером; в екосистемі FishAudio зазвичай використовуються GAN-моделі, наприклад HiFi-GAN, або власний декодер Firefly. В IndexTTS2 далі виконується етап акустичного моделювання, на якому генерується спектрограма, що перетворюється на аудіо попередньо навченим кодеком. У ранніх версіях для цього використовувався U-DiT (U-Net з дифузією), а в нових – Zipformer, сучасна архітектура, розроблена спеціально для обробки аудіо. Вона генерує спектрограму значно стабільніше, ніж U-DiT, і практично усуває пропуски слів або їх частин. Найслабшим місцем моделі є її авторегресійна природа: для визначення другого фрагмента аудіо модель має спочатку згенерувати перший і не може згенерувати сотий фрагмент, доки не завершить дев'яносто дев'ятий. Через таку строгу послідовність процес неможливо розпаралелити.

4. Лінгвістика та якість синтезу української мови

Можливість якісного тонкого налаштування для української мови критично залежить від лінгвістичних знань, закладених у модель під час попереднього навчання (pre-training). Робота з кириличним алфавітом, специфічними фонемами та правилами наголошування потребує наявності відповідних закономірностей у вагах моделі (для української мови – зокрема пом'якшення приголосних).

Для характеристики здатності моделі працювати з кирилицею використовують термін «крослінгвальний потенціал». Оскільки більшість розглянутих моделей попередньо навчено переважно на англійській та китайській мовах, цей потенціал у них суттєво різниться.

4.1 OmniVoice

Серед розглянутих моделей OmniVoice має найширше лінгвістичне охоплення: вона офіційно підтримує понад 600 мов, що є найбільшим показником серед сучасних моделей zero-shot синтезу мовлення. Українська мова входить до цього переліку. Базову модель навчено на безпрецедентному за обсягом наборі відкритих даних – 581 000 годин.

Для навчання zero-shot синтезу (тобто відтворення голосу за коротким референсним записом) під час попереднього навчання моделі потрібні терабайти даних. Однак близько 90 % доступних якісних аудіоданих в інтернеті припадає на англійську, китайську та іспанську мови. Українська, як і сотні інших мов, належить до низькоресурсних (low-resource), тобто чистих розмічених наборів даних для неї існує значно менше. За класичного підходу до навчання OmniVoice, найімовірніше, синтезувала б українське мовлення з англійським (чи китайським) акцентом, пропусками звуків і неправильним пом'якшенням приголосних. Для запобігання погіршенню якості для української та інших низькоресурсних мов під час навчання OmniVoice застосовується стратегія передискретизації даних на рівні мов (language-level data resampling). Її суть полягає у штучному збільшенні частки даних низькоресурсних мов за допомогою коефіцієнтів повторення, що дозволяє збалансувати вплив різних мовних груп на градієнтні оновлення моделі. Завдяки ініціалізації з LLM та наявності української мови в навчальному корпусі (зокрема з джерел FLEURS та Common Voice) OmniVoice має стійке уявлення про українську фонетику. З огляду на успішне донавчання моделі для інших низькоресурсних мов можна стверджувати, що її архітектура здатна до глибокого крослінгвального узагальнення: навіть за невеликого обсягу українських даних модель використовує акустичні закономірності споріднених слов'янських мов, зберігаючи правильну вимову. Це робить OmniVoice оптимальним кандидатом для донавчання: модель не потрібно навчати кирилиці з нуля, достатньо адаптувати її до конкретного голосу та усунути незначні акцентні артефакти.

4.2 Fish Speech S2

За заявою авторів, FishAudio2 (Fish Speech) також розроблялася з метою максимального мовного охоплення. В офіційній документації заявлено підтримку української мови (uk) поряд з російською (ru), польською (pl) та іншими європейськими мовами. Навчальний корпус моделі перевищує 720 000 годин багатомовного аудіо, що забезпечує глибоке моделювання акустичних і просодичних особливостей різних мов. Варто відзначити наявність успішних прецедентів тонкого налаштування Fish Speech 1.5, зокрема для української мови: автори повідомляють про донавчання моделі на власному наборі даних обсягом 240 годин чистого українського мовлення. Водночас результати власного тестування та повідомлення користувачів, які створювали голоси для споріднених кириличних мов (зокрема болгарської), свідчать про ризики поверхневого донавчання. Модель (подібно до IndexTTS2) схильна генерувати мовлення з яскраво вираженим російським акцентом, оскільки російськомовний сегмент у базовому наборі даних значно переважає. Щоб уникнути цього, розробники рекомендують під час донавчання обов'язково додавати тег [uk] до кожного текстового файлу транскрипції (.lab). Це змушує модель зафіксувати відповідний фонетичний простір і не звертатися до російськомовних акустичних векторних представлень.

Якість синтезу Fish Speech загалом оцінюється як надзвичайно висока: показник WER (Word Error Rate, частка помилково розпізнаних слів) становить близько 3.5% (для англійської мови).

4.3 Qwen3-TTS

Лінгвістична база моделі Qwen3-TTS є найбільш компромісною в контексті цього дослідження. Згідно з офіційною специфікацією, базова модель охоплює лише 10 основних мов: китайську, англійську, японську, корейську, німецьку, французьку, російську, португальську, іспанську та італійську. Відсутність української мови в офіційному переліку є суттєвим недоліком моделі для поставленої задачі. На перший погляд наявність російської мови серед підтримуваних мала б гарантувати коректну обробку кириличних символів токенізатором. Проте, як засвідчили тести, модель не знає унікальних українських літер («ї», «і», «є», «ґ») та специфічних для української мови фонетичних переходів. Під час спроби синтезувати український текст базовою моделлю без модифікацій інференс або завершувався помилкою розпізнавання невідомих токенів, або отримане аудіо мало виражений неприродний акцент. Можна припустити, що випуск двох версій моделі – легкої Qwen3-TTS-12Hz-0.6B-Base та більшої 1.7B-Base – мав на меті забезпечити можливість якісного розширення системи на нові мови. Оскільки модель навчено на 5 млн годин аудіо, її архітектура, імовірно, має високу здатність до моделювання мови. Тонке налаштування Qwen3 для української мови є цілком можливим, проте потребуватиме значно більшого набору даних (для повноцінного навчання нових фонем, а не лише адаптації голосу), ніж для інших розглянутих моделей, зокрема OmniVoice. Для часткового розв'язання проблеми доцільно застосовувати транслітерацію або фонемне перетворення тексту в IPA (International Phonetic Alphabet, Міжнародний фонетичний алфавіт) перед подачею в модель. При цьому доцільніше спиратися не на досвід IndexTTS2, яку навчали виключно на фонемах, а на досвід F5-44, яку навчали на гібридному наборі даних, що поєднує графемні та фонемні представлення.

5 Параметри використання моделей у експлуатації (production)

5.1 Клонування голосу та вихідні аудіохарактеристики

Для багатьох сценаріїв використання критично важливою є здатність моделі генерувати звук із заданим тембром (клонування) або створювати нові голоси за описом (дизайн голосу), а також якість вихідного аудіо, що визначається частотою дискретизації.

OmniVoice. OmniVoice генерує вихідне аудіо з частотою дискретизації 24 кГц (типове значення для сучасних T2S (text-to-speech) моделей). Модель має сучасні можливості zero-shot клонування голосу без додаткового донавчання: для цього достатньо референсного аудіо тривалістю 3–10 с.

Модель також має функцію автоматичної транскрипції референсного аудіо за допомогою вбудованої моделі Whisper (якщо текст референсного запису не надано вручну); ця функція вже стала стандартною для багатьох систем (наприклад, F5) і спрощує автоматизацію процесів. Окрім клонування, OmniVoice має потужну підсистему Voice Design, що дозволяє створювати нові голоси, задаючи в текстовому описі такі атрибути, як стать, вік, висота голосу та акцент. Для випадкового вибору голосу підсистема підтримує режим Auto Voice.

Qwen3-Audio. Моделі сімейства Qwen3-TTS (включно з модифікаціями Base, CustomVoice та VoiceDesign) також синтезують аудіо з частотою 24 кГц.

Qwen3 здатна практично миттєво виконувати zero-shot клонування голосу за референсним записом тривалістю 3 с. Як і OmniVoice, модель підтримує створення голосу за текстовим описом, що дозволяє гнучко генерувати нові голоси без референсних записів.

Fish Speech S2. Серед розглянутих моделей FishAudio2 (зокрема версія S2 Pro) вирізняється найвищою частотою дискретизації вихідного аудіо – 44,1 кГц, що забезпечує студійну якість звучання без обмеження високих частот. Для точного та стабільного клонування голосу без донавчання модель потребує референсного аудіо більшої тривалості – від 10 до 30 с.

Унікальною можливістю архітектури є нативна мультидикторна генерація (multi-speaker generation): модель дозволяє використовувати різні голоси в межах одного контекстного вікна (тобто одного запиту) для створення складних діалогів. При цьому не виникає затримок, пов'язаних з перемиканням моделей чи перезавантаженням ваг.

5.2 Гранулярне керування параметрами акустичної генерації

Можливість детермінованого керування інференсом є критичною вимогою для сучасних систем дубляжу, створення аудіокниг, інтерактивних голосових агентів тощо. Вимоги щодо керування тривалістю, швидкістю та емоційно-стилістичними характеристиками мовлення значною мірою розкривають фундаментальні відмінності між моделями.

5.2.1 Керування тривалістю та швидкістю інференсу

Керування тривалістю синтезованого аудіо та точний контроль темпу мовлення є найслабшим місцем більшості AR-систем, оскільки вони генерують звук токен за токеном без глобального контролю.

З огляду на це OmniVoice є беззаперечним лідером за цим критерієм. Завдяки неавторегресійній архітектурі модель має доступ до повного контексту послідовності під час ітеративного розмаскування. Аналіз програмного коду свідчить, що на рівні офіційного API (Application Programming Interface, прикладний програмний інтерфейс) (через клас OmniVoiceGenerationConfig або параметри функції model.generate()) користувачам і дослідникам доступні два параметри: duration та speed. Параметр duration (тип float) дозволяє задати фіксовану тривалість вихідного аудіо в секундах. Наприклад, якщо фразу необхідно озвучити рівно за 10,0 с для точної відповідності часовим міткам, модель адаптує внутрішній темп мовлення для досягнення цієї мети; цей параметр має найвищий пріоритет і повністю перекриває інші налаштування швидкості. Параметр speed (тип float) працює як коефіцієнт (аналогічно F5): значення > 1.0 пришвидшує темп, а < 1.0 – уповільнює його.

Ще однією важливою можливістю керування тривалістю є автоматичне розбиття дуже довгих текстів (наприклад, для аудіокниг) на сегменти за допомогою параметрів audio_chunk_duration (за замовчуванням 15.0 с) та audio_chunk_threshold, що гарантує стабільне споживання VRAM незалежно від обсягу вхідного тексту. Подібний підхід реалізовано також у F5.

Qwen3-Audio також підтримує керування швидкістю, проте відповідні механізми реалізовано інакше. Офіційні API-сервери (зокрема розширення vLLM-Omni або власні реалізації на основі FastAPI) дозволяють передавати параметр speed у діапазоні від 0.25 до 4.0. Цей параметр суттєво впливає як на

швидкість синтезу, так і на темп відтворення. Qwen3 має ще один підхід до керування швидкістю, що ґрунтується на семантичному контролі: модель здатна інтерпретувати текстові інструкції (наприклад, «читай повільніше») й адаптувати темп на рівні генерації токенів. Для цього використовується алгоритм ARIA (Adaptive Rate Interleave Alignment), який динамічно узгоджує одиниці тексту та мовлення, мінімізуючи нестабільність, що виникає через різну ефективність кодування модальностей. Детальний аналіз цього алгоритму є перспективним напрямом подальших досліджень.

FishAudio2 має найменше засобів керування тривалістю. Аналіз запитів у репозиторії GitHub свідчить, що у відкритому вихідному коді (Fish Speech S2/1.5, остання версія станом на 19.06) базові інструменти інференсу не підтримують параметрів швидкості чи тривалості, хоча хмарний API компанії Fish Audio такий параметр підтримує. Відповідно, локальні розгортання моделі завжди генерують мовлення зі стандартним темпом, і для його зміни доводиться застосовувати сторонні алгоритми постобробки (Time-Scale Modification). Це неминуче призводить до погіршення якості звуку, спотворення фази та появи роботизованих артефактів.

Варто також відзначити, що похідна модель IndexTTS 2.5 є першою AR-моделлю з керованою тривалістю, тоді як базова Fish Speech у поточній версії є вкрай обмеженою в цьому аспекті.

5.2.2 Емоції та стилістика

Вимога до емоційної виразності (expressiveness) є обов'язковою для створення природних діалогів. Традиційно FishAudio2 вважається однією з найсильніших моделей емоційного синтезу. Використання LLaMA як базової моделі дозволяє їй глибоко враховувати семантику тексту. У моделі реалізовано механізм так званих «м'яких інструкцій» (soft instructions) у формі текстових описів, що дозволяє користувачеві задавати бажані емоційні стани (смуток, гнів, радість) під час інференсу. Водночас під час донавчання нового голосу може виникати така проблема: якщо референсний набір даних містить акустичні мітки стилів (наприклад, [whisper]), модель може жорстко пов'язувати ці теги емоцій виключно з конкретним диктором, втрачаючи здатність переносити відповідні емоції на інші голоси. Qwen3-Audio реалізує якісно новий підхід до керування емоціями. Завдяки мультимодальній архітектурі Thinker-Talker, описаній вище, модель підтримує наскрізний контроль емоцій та просодії через системні інструкції (промпти). Наприклад, передавши інструкцію «говори схвильовано, з паузами», користувач отримує відповідний акустичний ефект. Серед відомих авторам моделей аналогічних можливостей не виявлено. Qwen3-TTS здатна адаптивно налаштовувати тон і ритм не лише на основі явної інструкції, а й з опорою на семантичне розуміння самого тексту. При цьому модель коректно визначає, що окремі слова потребують іронічного чи сумного тону (це перевірено на російськомовних текстах). OmniVoice реалізує емоційний контроль через систему Voice Design, описану в розділі про клонування голосу. Замість клонування наявного голосу користувач може створити новий, задавши деталізовані атрибути: gender (стать), age (вік), pitch (висота тону), dialect (акцент) та style (наприклад, whisper). Окрім глобальних стилів, OmniVoice забезпечує високий рівень

точкового контролю (fine-grained control), який реалізовано шляхом вставлення невербальних символів безпосередньо в текст. Підтримуються, зокрема, теги [laughter] (сміх), [sigh] (зітхання), [surprise-oh] (здивування). Така можливість є критично важливою для генерації природних діалогів. Корисною є також можливість виправлення помилок вимови шляхом прямого вставлення фонем зі словника у квадратних дужках. Для української мови це ефективний інструмент роботи зі складною лексикою та запозиченнями.

5.3 Продуктивність та обчислювальна ефективність

Усі наведені далі значення отримано на інстансі AWS (Amazon Web Services) з чотирма графічними процесорами T4 (по 16 ГБ) без будь-якої оптимізації інференсу. Продуктивність синтезу оцінюють за двома основними метриками: затримкою першого пакета (Time-to-First-Audio, TTFA), що характеризує час холодного старту для потокових застосунків, та коефіцієнтом реального часу (Real-Time Factor, RTF) для офлайн-генерації. Значення RTF < 1,0 означає, що інференс виконується швидше за реальний час. OmniVoice є беззаперечним лідером за показником RTF, що зумовлено неавторегресійною архітектурою, яка дозволяє генерувати всі токени паралельно. Завдяки цьому OmniVoice досягає RTF 0,025, тобто швидкість синтезу в 40 разів перевищує реальний час. Для додаткового пришвидшення на менш потужному обладнанні розробники пропонують зменшити кількість ітеративних кроків розмаскування num_step зі стандартних 32 до 16, що незначно знизить якість, але ще більше пришвидшить синтез. Параметри семплювання, такі як position_temperature та layer_penalty_factor, дозволяють налаштувати баланс між якістю та швидкістю генерації; їх вплив у цьому дослідженні експериментально не перевірявся. Qwen3-Audio, за заявою розробників, орієнтована на мінімізацію затримки TTFA для голосових асистентів. Розробники стверджують, що використання легких каузальних згорток дозволяє досягти теоретичної наскрізної затримки 234 мс у режимі холодного старту та 97 мс у потоковому режимі. У власних експериментах отримано значення, приблизно у 2–2,5 раза вищі. Також повідомляється, що завдяки оптимізаціям (Flash Attention 2, torch.compile) на графічних процесорах серії RTX 3090 модель досягає RTF близько 0,65–0,70 (такого рівня не вдалося досягти для моделі F5 з частотою 24 кГц на T4). FishAudio2 продемонструвала найнижчу швидкодію серед усіх розглянутих моделей. Великий обсяг параметрів (4,4 млрд для серії S2) робить авторегресійний синтез обчислювально затратним: швидкодія моделі більш ніж удвічі (залежно від довжини тексту) поступається Qwen3-Audio. За даними розробників, навіть на промисловому графічному процесорі NVIDIA A100 RTF становить 0,15–0,25, а на обладнанні середнього рівня (RTX 4060) зростає до 5, тобто генерація відбувається у 5 разів повільніше за реальний час. Тому на графічних процесорах Tesla T4 використання FishAudio2 в режимі реального часу неможливе, і модель придатна лише для офлайн-синтезу текстових масивів.

6. Підготовка наборів даних для донавчання моделей української мови

Якість кінцевого українського голосу залежить не лише від архітектури моделі, а й від суворого дотримання вимог до підготовки наборів даних. Кожна з розглянутих моделей використовує власний конвеєр підготовки даних.

6.1 Мінімальні обсяги наборів даних

Вимоги до мінімального обсягу набору даних для тонкого налаштування суттєво відрізняються залежно від того, чи підтримує базова модель відповідну мову. Qwen3-TTS: для базового клонування тембру диктора (LoRA) мінімально достатній обсяг даних становить близько 5 хв (приблизно 30 аудіофрагментів), тоді як оптимальний обсяг для стабільного голосу – 10–30 хв. Проте, оскільки модель не підтримує українську мову, такого обсягу вистачить лише для відтворення тембру; для навчання нових фонем та усунення вираженого акценту потрібен значно більший набір даних, обсяг якого оцінюється щонайменше у 100 годин. OmniVoice: модель уже добре володіє українською мовою. Для якісного донавчання, особливо під конкретного диктора зі стабілізацією вимови, розробники рекомендують використовувати щонайменше 10 годин чистого навчального аудіо. Зважаючи на обмежений досвід роботи з цією моделлю, у дослідженні орієнтуємося на подвоєне значення – 20 годин. FishAudio2 (Fish Speech): офіційні рекомендації для базового донавчання передбачають мінімальний обсяг набору даних понад 1 годину. Проте практичний досвід свідчить, що для подолання російського акценту необхідно або використовувати набори даних обсягом близько 200–300 годин, або застосовувати двоетапний підхід (50 годин загального українського аудіо + 20 годин цільового диктора).

6.2 Qwen3-TTS

Підготовка набору даних для сімейства Qwen3 є найбільш вимогливою, оскільки ця модель найсуворіше регламентує технічні параметри. Основною вимогою є частота дискретизації аудіо 24 кГц. Аналіз коду свідчить, що за частоти вхідного аудіо 16 кГц конвеєр генерації кодеків не виявляє цю невідповідність на початку, а видає помилку AssertionError уже в процесі навчання, що призводить до втрати часу. Цю проблему спостерігали у версіях 2 і 3. Отже, усі аудіофайли необхідно попередньо передискретизувати до 24 кГц. Формат даних передбачає створення файлу JSONL (JSON Lines – формат, у якому кожен рядок містить окремий об'єкт JavaScript Object Notation), де кожен об'єкт містить шляхи до цільового аудіо (audio), транскрипцію (text), еталонне аудіо диктора (ref_audio) та ідентифікатор диктора (speaker). Далі запускається скрипт prepare_data.py, який за допомогою токенізатора Qwen3-TTS-Tokenizer-12Hz перетворює вихідне аудіо на багатокодові представлення audio_codes і створює новий маніфест train_with_codes.jsonl. Інструкції розробника наголошують на необхідності видалення з транскрипцій будь-яких немовленнєвих тегів (наприклад, анотацій сміху), оскільки вони порушують роботу механізму навчання векторних представлень диктора. Крім того, додавання рівно 1 с тиші в кінець кожного навчального аудіофрагмента є критичним для уникнення аномального прискорення мовлення наприкінці згенерованих фраз під час інференсу.

6.3 OmniVoice

OmniVoice використовує формат зберігання WebDataset, який є фактичним стандартом для навчання великих моделей, оскільки суттєво зменшує навантаження на підсистему введення-виведення (disk I/O, input/output). Дані зберігаються не у вигляді тисяч окремих WAV-файлів (Waveform Audio File

Format): натомість користувач формує вихідний файл data.lst або JSONL з абсолютними шляхами до аудіо та транскрипціями.

Подальший опис наведено за документацією репозиторію розробників. Необхідно запустити скрипт extract_audio_tokens, який обробляє аудіо, перетворює його на масиви тензорів .npy та пакує у великі tar-архіви (шарди), кожен з яких містить тисячі векторів. Паралельно для кожного шарду генеруються файли метаданих JSONL. Такий підхід забезпечує максимальну пропускну здатність під час читання даних з диска в процесі розподіленого навчання.

6.4 FishAudio2

Для Fish Speech підготовка даних передбачає наявність аудіофайлів та відповідних транскрипцій у форматі .lab. Для уникнення змішування з російською фонетикою важливо явно додавати мовний тег (наприклад, [uk]) на початок кожного .lab-файлу під час навчання, що допомагає моделі сформувати правильні внутрішні асоціації.

7. Донавчання моделей на кластері з чотирьох графічних процесорів Tesla T4

У цій частині дослідження проаналізовано можливість донавчання моделей на конкретному апаратному забезпеченні – інстансі AWS, що містить чотири серверні графічні процесори NVIDIA Tesla T4.

7.1 Апаратні обмеження архітектури Tesla T4

На основі наявного досвіду оптимізації інференсу моделі F5 на T4 можна сформулювати основні обмеження цієї архітектури.

Tesla T4 побудована на архітектурі NVIDIA Turing (обчислювальна можливість sm_75). Кожен графічний процесор має 16 ГБ відеопам'яті GDDR6 (Graphics Double Data Rate 6) та 320 тензорних ядер Turing. На момент виходу це був потужний прискорювач, проте в контексті сучасного навчання аудіомоделей він має три критичні недоліки.

1. Обмежений обсяг VRAM: 16 ГБ на один графічний процесор недостатньо для повного (full-parameter) донавчання моделей з мільярдами параметрів. Це змушує застосовувати методи параметрично-ефективного донавчання (Parameter-Efficient Fine-Tuning, PEFT), зокрема LoRA (Low-Rank Adaptation), та/або алгоритми шардингу станів оптимізатора DeepSpeed ZeRO-2/3 (останній застосовувався під час навчання IndexTTS2).

2. Відсутність підтримки BFloat16: архітектура Turing апаратно не підтримує формат даних bfloat16, який є стандартом для сучасних трансформерів завдяки широкому динамічному діапазону. Це змушує навчати моделі або в менш стабільному форматі float16 (з ризиком зникнення градієнтів), або в повільнішому float32.

3. Обмежений обсяг розподіленої пам'яті: на кожен потоковий мультипроцесор T4 припадає близько 64–99 КБ розподіленої пам'яті (shared memory) на блок. Це обмеження є ключовою проблемою для сучасних реалізацій ядер механізму уваги (attention kernels).

7.2 OmniVoice

Тонке налаштування OmniVoice на кластері Tesla T4 на перший погляд є оптимальним варіантом, оскільки модель має лише 0,6 млрд параметрів і легко

вміщується в 16 ГБ VRAM. Проте, як свідчать документація та програмний код, стандартний навчальний конвеєр OmniVoice жорстко прив'язаний до оптимізованого ядра flex_attention (з компілятором Triton), призначеного для обробки упакованих послідовностей. У режимі навчання ядро flex_attention автоматично налаштовується на розмір блоку (наприклад, 128×128), що потребує близько 128 КБ розподіленої пам'яті на один потоковий блок. Оскільки T4 має обмеження 99 КБ на блок, спроба запустити стандартний скрипт run_finetune.sh, найімовірніше, завершиться помилкою ядра Triton. Аналогічна проблема виникає на всіх графічних процесорах, крім прискорювачів рівня A100 та H100, де обсяг розподіленої пам'яті становить 164 КБ і більше. Тому розробники моделі передбачили резервний механізм (fallback) – підтримку стандартного Scaled Dot-Product Attention (SDPA) під час навчання. Такий підхід широко застосовується в трансформерних моделях з обмеженнями щодо розподіленої пам'яті. Ініціалізувавши модель з параметром attn_implementation="sdpa", можна повністю обійти обмеження пам'яті Triton. Отже, завдяки цьому механізму донавчання OmniVoice на кластері з чотирьох T4 є можливим, а з урахуванням невеликого розміру моделі та швидкого завантаження даних через WebDataset – ще й достатньо швидким та ефективним.

7.3 Qwen3-TTS

Для моделі Qwen3-TTS (версія 1.7B) обсяг ваг у 16-бітному форматі перевищує 3,4 ГБ, що разом із градієнтами та станами оптимізатора Adam наближається до межі 16 ГБ VRAM одного T4 (за необхідності можна використати квантований варіант Adam, який потребує значно менше пам'яті). Навчання можливе із застосуванням LoRA та паралелізму даних на чотирьох графічних процесорах за допомогою DeepSpeed ZeRO-2 (розробники також згадують фреймворк ms-swift). Для уникнення помилок нестачі пам'яті (Out-Of-Memory, OOM) на T4 під час обробки довгих аудіофрагментів доцільно встановити мінімальний розмір пакета (batch_size = 1 або 2) і компенсувати це накопиченням градієнтів (grad_accum = 16 або 32). Такий підхід уже застосовувався під час фонемного навчання IndexTTS2. Головним викликом під час роботи з Qwen3-TTS є наявність критичних алгоритмічних помилок в офіційних скриптах донавчання (зокрема sft_12hz.py), які необхідно виправити перед запуском процесу на українському наборі даних. З огляду на їх важливість, нижче наведено ці помилки та способи їх усунення.

1. Помилка подвійного зсуву міток (double label-shift): офіційний скрипт самостійно зсуває мітки цільових токенів, а вбудована функція втрат ForCausalLMLoss бібліотеки HuggingFace робить це повторно. Така розбіжність між навчанням та інференсом призводить до того, що з кожною епохою згенероване мовлення стає неконтрольовано швидким і нерозбірливим. Помилку усуває пряма заміна на функцію F.cross_entropy().
2. Відсутність виклику text_projection: у базовому коді відсутня проєкція векторних представлень тексту в простір ознак модуля Talker. Текстові вектори подаються без перетворення, що погіршує якість навчання.
3. Некоректна швидкість навчання (learning rate, LR): стандартне значення LR = 2e-5 є занадто високим для моделі 1.7B і спричиняє руйнування токенів

кінця послідовності (end of sequence, EOS), унаслідок чого модель безперервно генерує фоновий шум. Тому рекомендовано використовувати LR = 2e-6 та обмежити навчання 10 епохами.

Після внесення цих виправлень донавчання Qwen3 на чотирьох T4 має бути успішним.

7.4 FishAudio2

Детальне вивчення моделі дозволяє стверджувати, що донавчання Fish Speech (4,4 млрд параметрів) на кластері з чотирьох Tesla T4 є надзвичайно ресурсозатратним. Розмір моделі вимагає обов'язкового використання LoRA-адаптерів виключно для компонента LLaMA. Досвід донавчання для болгарської мови свідчить, що навчання базової моделі впродовж 500 епох з розміром пакета 32 займає близько 44 годин на значно потужнішому графічному процесорі NVIDIA V100. Використання чотирьох T4 забезпечить паралелізм даних (Distributed Data Parallel), однак відсутність високошвидкісного інтерфейсу NVLink між графічними процесорами спричинить значні затримки синхронізації градієнтів через шину PCIe (Peripheral Component Interconnect Express). Відповідно, повноцінне донавчання для української мови може тривати кілька тижнів інтенсивних обчислень. Необхідно також навести застереження розробників, зазначене в документації: не рекомендується виконувати донавчання версій моделі, які пройшли етап навчання з підкріпленням (RL), оскільки це спричиняє зсув розподілу (distribution shift) і неминуче погіршення якості генерації.

8. Висновки та рекомендації

Узагальнені результати аналізу технічних характеристик, лінгвістичних можливостей та апаратних обмежень розглянутих моделей щодо задачі донавчання для української мови наведено в таблиці 1. На основі отриманих результатів можна стверджувати, що найбільш придатною для донавчання моделі української мови на кластері з чотирьох графічних процесорів Tesla T4 є OmniVoice. Її дифузійна неавторегресійна архітектура забезпечує точне керування тривалістю та швидкістю мовлення (duration / speed), що є однією з обов'язкових вимог, яка в інших розглянутих моделях не виконується або виконується частково. Базова підтримка понад 600 мов, зокрема української, створює потужне лінгвістичне підґрунтя, що мінімізує появу російського акценту завдяки глибоким крослінгвальним зв'язкам LLM. Компактний розмір (0,6 млрд параметрів) забезпечує найвищу швидкість інференсу. Єдиною проблемою є технічне обмеження архітектури T4 (недостатній обсяг розподіленої пам'яті для ядра Triton flex_attention), яке долається завдяки офіційно підтримуваному переходу на SDPA.

Qwen3-TTS є вагомою альтернативою, зокрема для створення діалогових агентів, завдяки найкращому розумінню емоційних інструкцій (через системні промпти). Її тонке налаштування на T4 можливе за допомогою LoRA та ZeRO-2. Однак відсутність нативної підтримки української фонетики вимагає формування значно більшого набору даних для навчання нових фонем з нуля. Крім того, наявність серйозних помилок у навчальних скриптах (подвійний зсув міток) потребуватиме корекції коду та суворого контролю частоти дискретизації (24 кГц).

Таблиця 1

Лінгвістичні можливості та апаратні обмеження розглянутих моделей щодо задачі донавчання для української мови

Критерій оцінки	OmniVoice	Qwen3-Audio (TTS/Omni)	FishAudio2 (Fish Speech)
Архітектурна база	NAR дифузійна (~0,6 млрд)	Авторегресійна MoE (0,6 / 1,7 млрд)	Подвійна авторегресійна (4,4 млрд)
Охоплення мов / українська	600+ мов. Високий крос-лінгвальний потенціал для кирилиці.		Підтримка 80+ мов, наявність тегу [uk]. Існують українські моделі.
Вихідна частота дискретизації	24 кГц	24 кГц	44,1 кГц (студійна якість)
Можливості клонування голосу	Zero-shot (3–10 с), Voice Design, автоматична транскрипція	Zero-shot (3 с), дизайн голосу за описом	Zero-shot (10–30 с), нативні мультидикторні діалоги
Мінімальний обсяг даних для донавчання	Від 10 годин (українська вже підтримується базово)	5–30 хвилин (тільки для тембру), сотні годин (для навчання української фонетики)	> 1 години (технічний мінімум), 50–240 годин (на практиці для української фонетики)
Точне управління тривалістю	Високе. Глобальні API-параметри duration та speed.	Середнє. Управління через семантичні системні промпти та ARIA.	Низьке. Параметр швидкості відсутній у відкритому коді.
Контроль емоцій	Voice Design, гнучкі невербальні теги ([laughter]).	Високий. Глибоке розуміння контексту тексту, системні інструкції.	Високий. Текстові інструкції для експресії.
Продуктивність інференсу (орієнтовні значення)	Екстремальна швидкість (RTF 0,025).	Висока (TTFA 97 мс, RTF ≈ 0,7).	Низька (RTF 0,2 на A100, у рази повільніше на T4).
Можливість донавчання на 4 × Tesla T4	Висока. Необхідна зміна коду на attn_implementation ="sdpa".	Середня. Потребує виправлення помилок у скриптах і мінімального розміру пакета.	Низька. Надзвичайно тривале навчання через 4,4 млрд параметрів та обмеження шини PCIe.
Критерій оцінки	OmniVoice	Qwen3-Audio (TTS/Omni)	FishAudio2 (Fish Speech)

Використання FishAudio2 (Fish Speech) для донавчання моделі української мови є найменш доцільним серед розглянутих варіантів. Попри найвищу якість генерації емоційного та виразного мовлення, а також доведену здатність працювати з кирилицею, відсутність вбудованого керування швидкістю генерації у відкритому коді є критичною перешкодою, зокрема для задачі дубляжу. Крім того, розмір 4,4 млрд параметрів зробить донавчання на Tesla T4 надзвичайно тривалим і ресурсно неефективним, що призведе до економічно невиправданих витрат часу на розробку.

Література

[1] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. In *Advances in Neural Information Processing Systems* (Vol. 30). Curran Associates. https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf

[2] Kong, J., Kim, J., & Bae, J. (2020). HiFi-GAN: Generative adversarial networks for efficient and high fidelity speech synthesis. In *Advances in Neural Information Processing Systems* (Vol. 33). Curran Associates. https://proceedings.neurips.cc/paper/2020/hash/c5d736809766d46260d816d8dbc9eb44-Abstract.html

[3] Kim, J., Kong, J., & Son, J. (2021). Conditional variational autoencoder with adversarial learning for end-to-end text-to-speech. In *Proceedings of the 38th International Conference on Machine Learning* (Vol. 139, pp. 5530–5540). PMLR. https://proceedings.mlr.press/v139/kim21f.html

[4] Zeghidour, N., Luebs, A., Omran, A., Skoglund, J., & Tagliasacchi, M. (2022). SoundStream: An end-to-end neural audio codec. *IEEE/ACM Transactions on Audio, Speech, and Language Processing, 30*, 495–507. https://arxiv.org/abs/2107.03312

[5] Défossez, A., Copet, J., Synnaeve, G., & Adi, Y. (2023). High fidelity neural audio compression. *Transactions on Machine Learning Research*. https://doi.org/10.48550/arXiv.2210.13438

[6] Wang, C., Chen, S., Wu, Y., Zhang, Z., Zhou, L., Liu, S., Chen, Z., Liu, Y., Wang, H., Li, J., He, L., Zhao, S., & Wei, F. (2023). *Neural codec language models are zero-shot text to speech synthesizers* (arXiv:2301.02111). arXiv. https://doi.org/10.48550/arXiv.2301.02111

[7] Seed Team. (2024). *Seed-TTS: A family of high-quality versatile speech generation models* (arXiv:2406.02430) [Technical report]. ByteDance. https://doi.org/10.48550/arXiv.2406.02430

[8]. Du, Z., Chen, Q., Zhang, S., Hu, K., Lu, H., Yang, Y., Hu, H., Zheng, S., Gu, Y., Ma, Z., Gao, Z., & Yan, Z. (2024). *CosyVoice: A scalable multilingual zero-shot text-to-speech synthesizer based on supervised semantic tokens* (arXiv:2407.05407). arXiv. https://doi.org/10.48550/arXiv.2407.05407

[9] Zhou, S., Zhou, Y., He, Y., Zhou, X., Wang, J., Deng, W., & Shu, J. (2026). IndexTTS2: A breakthrough in emotionally expressive and duration-controlled auto-regressive zero-shot text-to-speech. *Proceedings of the AAAI Conference on Artificial Intelligence, 40*(41), 35139–35148. https://doi.org/10.1609/aaai.v40i41.40820

[10] Eskimez, S. E., Wang, X., Thakker, M., Li, C., Tsai, C.-H., Xiao, Z., Yang, H., Zhu, Z., Tang, M., Tan, X., Liu, Y., Zhao, S., & Kanda, N. (2024). *E2 TTS: Embarrassingly easy fully non-autoregressive zero-shot TTS* (arXiv:2406.18009). arXiv. https://doi.org/10.48550/arXiv.2406.18009

[11] Chen, Y., Niu, Z., Ma, Z., Deng, K., Wang, C., Zhao, J., Yu, K., & Chen, X. (2024). *F5-TTS: A fairytaler that fakes fluent and faithful speech with flow matching* (arXiv:2410.06885). arXiv. https://doi.org/10.48550/arXiv.2410.06885

[12] Wang, Y., Zhan, H., Liu, L., Zeng, R., Guo, H., Zheng, J., Zhang, Q., Zhang, X., Zhang, S., & Wu, Z. (2025). MaskGCT: Zero-shot text-to-speech with masked generative codec transformer. In *Proceedings of the Thirteenth International Conference on Learning Representations (ICLR 2025)*. https://proceedings.iclr.cc/paper_files/paper/2025/hash/74a31a3b862eb7f01defbbed8e5f0c69-Abstract-Conference.html

[13] Chang, H., Zhang, H., Jiang, L., Liu, C., & Freeman, W. T. (2022). MaskGIT: Masked generative image transformer. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 11315–11325). IEEE. https://doi.org/10.1109/CVPR52688.2022.01103

[14] Zhu, H., Ye, L., Kang, W., Yao, Z., Guo, L., Kuang, F., Han, Z., Zhuang, W., Lin, L., & Povey, D. (2026). *OmniVoice: Towards omnilingual zero-shot text-to-speech with diffusion language models* (arXiv:2604.00688). arXiv. https://doi.org/10.48550/arXiv.2604.00688

[15] Liao, S., Wang, Y., Li, T., Cheng, Y., Zhang, R., Zhou, R., & Xing, Y. (2024). *Fish-Speech: Leveraging large language models for advanced multilingual text-to-speech synthesis* (arXiv:2411.01156) [Technical report]. Fish Audio. https://doi.org/10.48550/ arXiv.2411.01156

[16] Fish Audio Team. (2026). *Fish Audio S2 technical report* (arXiv:2603.08823) [Technical report]. Fish Audio. https://doi.org/10.48550/arXiv.2603.08823

[17] Xu, J., Guo, Z., He, J., Hu, H., He, T., Bai, S., Chen, K., Wang, J., Fan, Y., Dang, K., Zhang, B., Wang, X., Chu, Y., & Lin, J. (2025). *Qwen2.5-Omni technical report* (arXiv:2503.20215) [Technical report]. Alibaba Group. https://doi.org/10.48550/ arXiv.2503.20215

[18] Qwen Team. (2025). *Qwen3-Omni technical report* (arXiv:2509.17765) [Technical report]. Alibaba Group. https://doi.org/10.48550/arXiv.2509.17765

[19] Shazeer, N., Mirhoseini, A., Maziarz, K., Davis, A., Le, Q., Hinton, G., & Dean, J. (2017). Outrageously large neural networks: The sparsely-gated mixture-of-experts layer. In *Proceedings of the 5th International Conference on Learning Representations (ICLR 2017)*. https://openreview.net/forum?id=B1ckMDqlg

[20] Hu, H., Zhu, X., He, T., Guo, D., Zhang, B., Wang, X., Guo, Z., Jiang, Z., Hao, H., Guo, Z., Zhang, X., Zhang, P., Yang, B., Xu, J., Zhou, J., & Lin, J. (2026). *Qwen3-TTS technical report* (arXiv:2601.15621) [Technical report]. Alibaba Group. https://doi.org/ 10.48550/arXiv.2601.15621

[21] Ardila, R., Branson, M., Davis, K., Kohler, M., Meyer, J., Henretty, M., Morais, R., Saunders, L., Tyers, F., & Weber, G. (2020). Common Voice: A massively-multilingual speech corpus. In *Proceedings of the Twelfth Language Resources and Evaluation Conference* (pp. 4218–4222). European Language Resources Association. https://aclanthology.org/ 2020.lrec-1.520

[22] Conneau, A., Ma, M., Khanuja, S., Zhang, Y., Axelrod, V., Dalmia, S., Riesa, J., Rivera, C., & Bapna, A. (2023). FLEURS: Few-shot learning evaluation of universal representations of speech. In *2022 IEEE Spoken Language Technology Workshop (SLT)* (pp. 798–805). IEEE. https://doi.org/10.1109/SLT54892.2023.10023141

[23] Pratap, V., Tjandra, A., Shi, B., Tomasello, P., Babu, A., Kundu, S., Elkahky, A., Ni, Z., Vyas, A., Fazel-Zarandi, M., Baevski, A., Adi, Y., Zhang, X., Hsu, W.-N., Conneau, A., & Auli, M. (2024). Scaling speech technology to 1,000+ languages. *Journal of Machine Learning Research*, *25*(97), 1–52. https://jmlr.org/papers/v25/23-1318.html

[24] Radford, A., Kim, J. W., Xu, T., Brockman, G., McLeavey, C., & Sutskever, I. (2023). Robust speech recognition via large-scale weak supervision. In *Proceedings of the 40th International Conference on Machine Learning* (Vol. 202, pp. 28492–28518). PMLR. https://proceedings.mlr.press/v202/radford23a.html

[25] Hu, E. J., Shen, Y., Wallis, P., Allen-Zhu, Z., Li, Y., Wang, S., Wang, L., & Chen, W. (2022). LoRA: Low-rank adaptation of large language models. In *Proceedings of the Tenth International Conference on Learning Representations (ICLR 2022)*. https://openreview.net/forum?id=nZeVKeeFYf9

[26] Rajbhandari, S., Rasley, J., Ruwase, O., & He, Y. (2020). ZeRO: Memory optimizations toward training trillion parameter models. In *SC20: International Conference for High Performance Computing, Networking, Storage and Analysis*. IEEE. https://arxiv.org/abs/1910.02054

[27] Micikevicius, P., Narang, S., Alben, J., Diamos, G., Elsen, E., Garcia, D., Ginsburg, B., Houston, M., Kuchaiev, O., Venkatesh, G., & Wu, H. (2018). Mixed precision training. In *Proceedings of the Sixth International Conference on Learning Representations (ICLR 2018)*. https://arxiv.org/abs/1710.03740

[28] Dao, T., Fu, D. Y., Ermon, S., Rudra, A., & Ré, C. (2022). FlashAttention: Fast and memory-efficient exact attention with IO-awareness. In *Advances in Neural Information*

Processing Systems (Vol. 35). Curran Associates. https://proceedings.neurips.cc/paper_files/paper/2022/hash/67d57c32e20fd0a7a302cb81d36e40d5-Abstract-Conference.html

[29] Dong, J., Feng, B., Guessous, D., Liang, Y., & He, H. (2024). *Flex Attention: A programming model for generating optimized attention kernels* (arXiv:2412.05496). arXiv. https://doi.org/10.48550/arXiv.2412.05496

[30] Yao, Z., Guo, L., Yang, X., Kang, W., Kuang, F., Yang, Y., Jin, Z., Lin, L., & Povey, D. (2024). Zipformer: A faster and better encoder for automatic speech recognition. In *Proceedings of the Twelfth International Conference on Learning Representations (ICLR 2024)*. https://doi.org/10.48550/arXiv.2310.11230

FINE-TUNING SPECIFICS OF AUDIO-MODALITY LARGE LANGUAGE MODELS: OMNIVOICE, FISHAUDIO2 (FISHSPEECH S2) AND QWEN3 AUDIO

Dr.Sci., Peleshko D.[1], Peleshko S.-D.[2],
Dr.Sci., Vynokurova O.[3], Ph.D., Peleshko M.[4]
[1,3] Ivan Franko National University of Lviv,
[2] Ukrainian Catholic University,
[4] Lviv State University of Life Safety

Abstract. *Building high-quality Ukrainian speech synthesis systems is hindered by the low-resource status of the Ukrainian language and by limited available hardware. Modern audio-modal large language models achieve high-quality zero-shot synthesis, yet their fine-tuning for Ukrainian on mid-range graphics processing units (GPUs) remains insufficiently studied.* ***Objective.*** *To conduct a comparative study of OmniVoice, FishAudio2 (Fish Speech S2) and Qwen3-TTS in order to determine their fine-tuning capabilities for Ukrainian on a cluster of four NVIDIA Tesla T4 GPUs.* ***Methods.*** *We analysed the architectural paradigms of the models (non-autoregressive diffusion, dual autoregressive, and Thinker-Talker with mixture of experts), their linguistic coverage, control over speech duration, rate and emotion, inference performance, dataset preparation requirements, and the hardware constraints of the Turing architecture.* ***Results.*** *OmniVoice combines built-in Ukrainian support, precise duration and speed control and the highest inference speed (real-time factor, RTF, of 0.025); the shared-memory limitation of the flex_attention kernel on T4 can be bypassed by switching to Scaled Dot-Product Attention (SDPA). Qwen3-TTS provides the best emotion control via system prompts but requires a much larger dataset to learn Ukrainian phonetics and fixes to its training scripts. FishAudio2 produces the most expressive 44.1 kHz speech, but its 4.4 billion parameters and the absence of speed control in the open-source code make fine-tuning on T4 impractical.* ***Conclusions.*** *OmniVoice is recommended for fine-tuning a Ukrainian speech synthesis model on a Tesla T4 cluster; Qwen3-TTS is an alternative for dialogue agents provided an extended Ukrainian dataset is built.*

Key words: *speech synthesis; audio-modal large language models; fine-tuning; Ukrainian language; OmniVoice; Fish Speech; Qwen3-TTS; NVIDIA Tesla T4; voice cloning; speech duration control.*

Наукове видання

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ТА ЦИФРОВІ ТЕХНОЛОГІЇ

Монографія

Під наук. ред. проф. В. Вичужаніна

Укр. та англ. мовами

Підписано до друку 30.09.2026. Формат 60×84/16.
Папір офсетний. Гарнітура Times. Цифровий друк.
Ум.-друк. арк. 19,65. Тираж 300. Замовлення № 1026-89.
Віддруковано з готового оригінал-макета.

Українсько-польське наукове видавництво «Liha-Pres»
79000, м. Львів, вул. Технічна, 1

87-100, м. Торунь, вул. Лубіцка, 44
Телефон: +38 (050) 658 08 23
E-mail: editor@liha-pres.eu

Свідоцтво суб'єкта видавничої
справи ДК № 6423 від 04.10.2018 р.