Ivan Ivanets **Іван Іванець**	PhD student, Department of Computer Technologies in Publishing and Printing, Lviv Polytechnic National University, Lviv, Ukraine. https://orcid.org/0009-0004-7508-4867 e-mail: ivan.d.ivanets@lpnu.ua	аспірант, кафедра комп'ютерних технологій у видавничо-поліграфічних процесах, Національний університет "Львівська політехніка", Львів, Україна.
Volodymyr Ovsyak **Володимир Овсяк**	Professor, PhD, Professor at the Department of Computer Technologies in Publishing and Printing, Lviv Polytechnic National University, Lviv, Ukraine; Kielce University of Technology, Kielce, Poland. https://orcid.org/0000-0001-9295-284X e-mail: vovsyak@tu.kielce.pl	професор, д-р техн. наук, професор кафедри комп'ютерних технологій у видавничо-поліграфічних процесах, Національний університет "Львівська політехніка"; Kielce University of Technology, Kielce, Poland.
Oleksandr Ovsyak **Олександр Овсяк**	Associate Professor, PhD, Professor at the Department of Computer Science, Ukrainian National Forestry University, Lviv, Ukraine. https://orcid.org/0000-0003-2620-1938 e-mail: ovsjak@nltu.edu.ua	доцент, д-р техн. наук, професор кафедри комп'ютерних наук, Національний Лісотехнічний Університет України, Львів, Україна.

https://doi.org/10.31891/csit-2025-2-6
UDC 004.942

SIKORA Lubomyr, LYSA Nataliia, FEDEVYCH Olga, KHYLIAK Nazarii
Lviv Polytechnic National University

KEY ASPECTS FOR THE DEVELOPMENT OF INFORMATION AND MEASUREMENT SYSTEMS FOR DETERMINING ENVIRONMENTAL POLLUTION

The intensification of production at petrochemical, construction, industrial, and energy companies and the aging of equipment at major technological and energy facilities lead to increased emissions of toxic and dusty substances into the air, soil, and water. As a result of the ecosystem cycle, these chemical compounds enter the soil and water, causing pollution.

The main task of environmental expertise is to determine the degree of risk and safety of industrial activity, organize a program of expert assessment of industrial production facilities, establish compliance of facilities with the requirements of environmental legislation, examine the quality of natural resources, form a balance of quality criteria for the environmental safety of facilities and the environment, assess the negative impact of industrial and municipal structures on the environment, and expertly evaluate programs for the introduction of new technology.

Air monitoring is necessary to detect the effects of pollutants and their impact on: corrosion of structures, erosion of land resources, impact on human health, impact on flora and the environment, water pollution, and food contamination.

The article highlights the basic concepts for building information and measuring systems (laser concentrometer and opto-galvanic sensors) for rapid analysis of environmental pollution such as air, water, and soil in emergency and extreme situations. The air and water pollution was detected around energy facilities and various industrial production facilities that are at risk of military attack. The article describes the development and construction of a laser information and measurement system for measuring dust in the atmosphere and presents the results of a study of the chemical pollution of water wells in various industries.

Key words: sensor, information and measuring syste, monitoring, environment, pollution.

СІКОРА Любомир, ЛИСА Наталя, ФЕДЕВИЧ Ольга, ХИЛЯК Назарій
Національний університет «Львівська політехніка»

КЛЮЧОВІ АСПЕКТИ РОЗВИТКУ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМ ДЛЯ ВИЗНАЧЕННЯ ЗАБРУДНЕННЯ НАВКОЛИШНЬОГО СЕРЕДОВИЩА

Інтенсифікація виробництва на підприємствах нафтохімічної, будівельної, промислової та енергетичної галузей, а також старіння обладнання на великих технологічних та енергетичних об'єктах призводять до збільшення викидів токсичних і пилових речовин у повітря, ґрунт і воду. В результаті кругообігу речовин в екосистемі ці хімічні сполуки потрапляють у ґрунт і воду, спричиняючи їх забруднення.

Основним завданням екологічної експертизи є визначення ступеня ризику і безпеки промислової діяльності, організація програми експертної оцінки об'єктів промислового виробництва, встановлення відповідності об'єктів вимогам природоохоронного законодавства, експертиза якості природних ресурсів, формування балансу якісних критеріїв екологічної безпеки об'єктів і навколишнього середовища, оцінка негативного впливу виробничих і комунальних структур на навколишнє середовище, експертна оцінка програм впровадження нових технологій.

Моніторинг повітря необхідний для виявлення впливу забруднюючих речовин та їх впливу на: корозію споруд, ерозію земельних ресурсів, вплив на здоров'я людини, вплив на флору та навколишнє середовище, забруднення води, забруднення продуктів харчування.

У статті висвітлено основні концепції побудови інформаційно-вимірювальних систем (лазерний концентрометр та оптико-гальванічні сенсори) для експрес-аналізу забруднення навколишнього середовища - повітря, води та ґрунту - в аварійних та екстремальних ситуаціях. Виявлення забруднення повітря та води здійснювалося навколо енергетичних об'єктів та різних промислових виробництв, які знаходяться під загрозою військового нападу. У статті описано розробку та побудову лазерної інформаційно-вимірювальної системи для вимірювання пилу в атмосфері та наведено результати дослідження хімічного забруднення водозабірних свердловин у різних галузях промисловості.

Ключові слова: датчик, інформаційно-вимірювальна система, моніторинг, навколишнє середовище, забруднення.

Introduction

The second most important source after the intensification of production is the discharge of process water into water bodies and rivers from power plants and chemical and construction companies. One of the most powerful sources of emissions into the ecosystem after intensification is thermal power plants, which pollute the water and air of the environment.

Analysis of literature sources

Works [1,2,3] describe the conversion of fuel resources into energy resources using water as the basis of the conversion process, which is the carrier of thermal energy of fuel during combustion, into the kinetic energy of the turbine, which is transferred to the generator and converted into electricity. Channels and sensors for collecting data on the state of power unit units are also displayed and critical areas for their selection are identified.

To control the technological state of production processes and the environment, it is necessary to have a set of information and measurement systems that provide the selection of heterogeneous data from objects and the environment, assessment of state parameters, information technologies for interpreting images of situations

formulated from blocks of selected terminal data and identifying their intellectual content regarding the target state of the man-made production and environmental complex [3-8].

The works of world scientists [9-13] outline the main environmental problems in the construction of sensors for measuring environmental pollution.

Materials and methods

To develop environmental monitoring systems, both local and global, to assess the state of the environment and the impact on social infrastructure and living spaces, it is necessary to use modern scientific methods based on the basic principles of control theory to describe potentially hazardous objects with an aggregated hierarchical spatially dis-tributed structure, system analysis of energy management processes, mathematical logic, decision-making theory to build effective strategies for coordinating management in case of threats to the load mode and attacks at all levels of the hierarchy; theory of expert systems for assessing the situation and classifying data on the state of the environment around the object; methods of laser remote sensing theory for building photometers and information and measurement systems; data collection on the concentration of dust in the atmosphere and water solutions in the environment, both stationary and portable.

The problem of developing information systems for environmental assessment of the environment state around man-made facilities

The problems of monitoring the state of the ecosystem and socio-communal infrastructure in the presence of large industrial man-made energy-active complexes that are polluters are solved on the basis of new information-measurement technologies and the following tasks are being solved:

1. identification of sources and channels of environmental impact (industrial, domestic, natural) based on sampling;
2. development of data sampling tools and their accuracy, objectivity, reliability in relation to the target tasks based on information technologies;
3. improved information technologies for data processing and interpretation of the content of environmental situations based on the integration of systems;
4. development of a classification of situation methods based on expert assessments using databases, knowledge and expert systems in the structure of the DMSS (Decision making support systems);
5. development of data management and storage systems (DS - data storage, DDP - digital data processing);
6. development of primary and secondary standards for quality criteria and chemical pollutants (SO_2, NO_2, CO, O_3, Pb) and sampling for active ions $\left\langle SO_4^-, Cl^-, NH_4^+, NO_3^-, Ca^{++}, Mg^{++}, K^+ \right\rangle$ and components of radioactive fallout.

The monitoring tools are: sampling of water, air, compounds, methods of physical and chemical analysis and data processing, equipment for physical and chemical analysis, systematic interpretation of results.

The monitoring results form the basis for obtaining data and information on the components of the impact and their level: primary data from sensors and PCs, data on the physical and chemical composition of pollutants, assessment of the level and degree of danger of pollution impact on the environment, assessment of the composition and volume of pollution emissions.

Air pollutants include:

- gaseous inorganic substances $\left\langle SO_2, H_2S, NO_2, Cl_2, CO, SiF \right\rangle$;
- mineral acids $\left\langle HCl, HF, H_2SO_4, HNO_3 \right\rangle$;
- radionuclides (strontium, cesium, iodine, plutonium, radium);
- simple organic substances (formaldehyde, benzopyrene, etc.).

Water is an important vital and technological resource of natural origin. Safe, it is an essential resource for life, industrial and agricultural development, and therefore effective management of water consumption based on monitoring the state of water in the structure of the region's resources is necessary. As a link in the natural cycle, water is divided according to the source of the resource into: surface water, underground water (in rock stra-ta), and marine water (seas and oceans). A water body is a naturally formed or artificially created object, such as streams, swamps, rivers, underground springs, reservoirs, and seas.

For thermal power plants and the social sector, we classify the types of water use: special, non-special, and general.

Environmental status is an expression of the quality of the structure and functioning of water systems. It takes into account: the physical and chemical structure of water, characteristics and parameters of its flow, chemical state and level of pollution. A water quality standard is a set of water quality indicators that cannot be exceeded for the sake of human health and the ecosystem (limit values beyond which structural destruction of the system occurs). Water quality classes based on integral pollution are determined on the basis of the legal provisions of the Water Code (7 classes in Germany). Water monitoring systems are classified according to the type of water: natural, waste, and saline.

In order to make informed management decisions in the field of environmental protection, it is necessary to create an information and measurement distributed mul-ti-parameter system, as well as a bank of environmental and technological data in the structure of an expert decision support system for process control.

Methods for assessing the level of concentration of harmful impurities and dust in the technological and atmospheric environment using laser sensing

The method of controlling the atmospheric pollution by combustion products from thermal power plants and dust from the construction industry by laser sensing is shown in Fig. 2.

Depending on the level of dust concentration and its dispersion, the laser beam is scattered and the power is reduced, while the level of losses depends on the dust concen-tration and its structure, which accordingly requires the construction of appropriate scales for assessing the parameters of the dust environment.

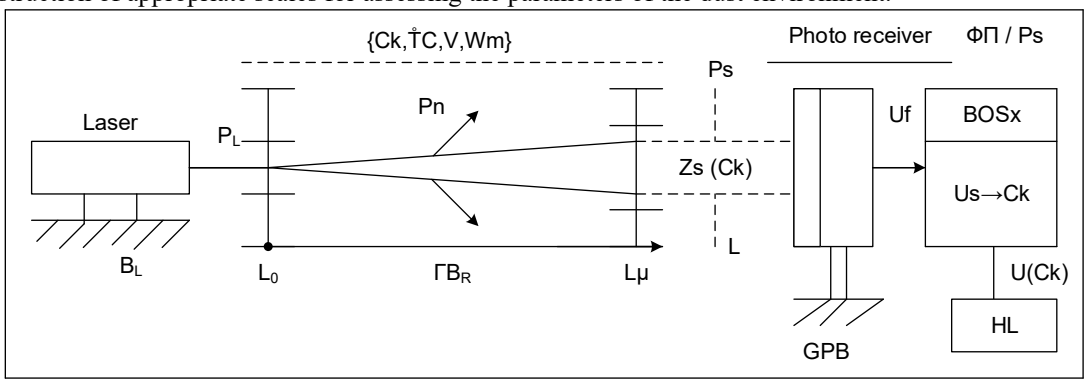


Figure 2. Scheme of laser sensing of dust pollution of the environment of man-made systems with indus-trial waste

Symbols in the diagram: B_L - geometric basis of the laser, P_L - laser power, L_0, L_μ - basis of the geometric environment with contamination $ГB_R(L_0, L_\mu)$;

P_S - beam power at the output of the control area, P_n - power of the scattered laser beam, GPB - geometric basis of the photodetector $(ФП / P_S)$, $U_f(Z_S)$ - voltage of the laser signal at the output of the photodetector after the processing of the probing beam $Z_S(C_K)$, $BOS_{ФП}(U_S \to C_K)$ - photodetector signal processing unit for information transformation in order to assess the concentration of air pollution by emissions of process products in the control area.

Methods of laser diagnostics of high-temperature coal dust and combustion products flows in power units of thermal power plants

An important problem is to control the level of concentration of coal dust flows into boilers after coal mills and the concentration of combustion products at the outlet, when they are sent to the chimney system.

Coal from different deposits has a ballast rock, which makes up (from 5% to 45%) of the content. When grinding in mills, coal dust is fed into recuperators to heat the stream (400-900^{0}C) before entering the boiler furnace. Changes in the composition of coal dust lead to a decrease in the level of useful content and a decrease in energy activity. When the concentration of the ground coal content changes, dynamic concentration emissions occur $\{C_i\}$, which can lead to an accident.

The requirements for controlling the concentration of the high-temperature mixture are satisfied by laser methods of remote sensing of the process medium through optical windows in dust ducts. The laser method of concentration control in the continuous mode of the gas-dust mixture flow in the dust ducts of power units is based on the estimation of laser beam losses due to photon scattering on dust particles moving in the dust duct flow during its transverse sensing through optical windows. Such windows are embedded in the cross-section of the dust duct and are permeable to a laser beam passing through the flow of a dust-gas mixture of fuel combustion products in the power unit boiler, which can change when passing through the recuperator within the limits of (300-600)^{0}C.

Fig. 3 shows a diagram of the process and structure of the laser sensing system for high-temperature coal dust entering the power unit boiler from the mills.

The notation in the diagram of Fig. 3:

SGm - specified generator with laser modulation frequency $(f_\mu = 625Hz)$;

PI - pulse amplification unit for powering a semiconductor laser (red spectrum $\lambda = 680n\mu$;

L_Z - laser emitter;

RN - ranking unit of evaluation normalization;

BDP - a laser signal amplification unit from the photodetector, which separates the concentration level component after processing the modulated signal $(Z_S(t,\tau,f)\to U_S(f,t,\xi_t))$ under the influence of an interference (ξ_t);

BAS - a unit for displaying the concentration level based on the balance method and alarming the level exceedance based on the assessment $(U(C_K))$.

In accordance with the method of sensing the environment (direct, reflected beam), a characteristic model is determined for ranking and assessing the concentration level of the high-temperature coal dust flow in the dust pipe of the power unit boiler.

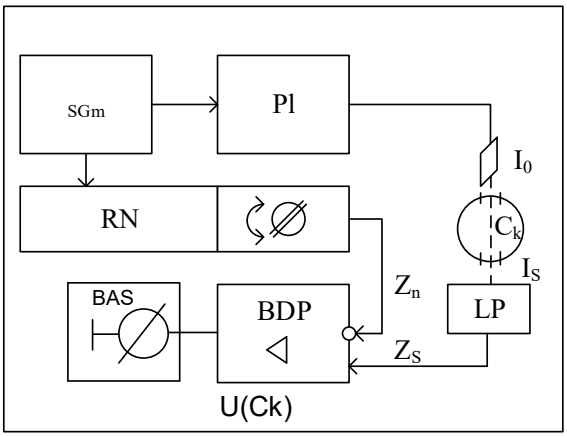


Figure 3. Diagram of the process of sounding the dust pipeline of the power unit

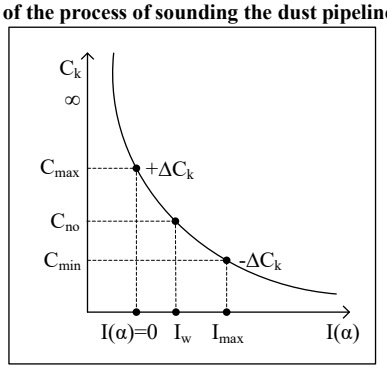


Figure 4. Characterization model for estimating the level of dust and impurities Concentration

The estimation of the intensity (energy) of the scattered laser beam of the corresponding concentration level at the output of the optical window in the dust pipe is based on the measurement transformations of the laser sensing signal (Fig. 3, 4):

- beam energy conversion during laser sensing: $I_s(t,S_c)=I_0\exp(-\alpha L(C_K,S_L))$
- selection of information about the dust concentration in the control area: $\exp(-\varphi_c(\alpha,S_e,C_K))=I_s(t,S_e)\cdot I_0^{-1}$
- determination of the dust concentration function after processing the scattered signal by dust: $\varphi_c(\alpha,S_e,C_k)=\ln(I_S(t,S_e)/I_0)=-\ln I_S(t,S_e)+\ln I_0=\Delta\ln(\psi(I_S,I_0))$;
- evaluation of the imbalance of the level of dust concentration in the dust wires is formed in the rank discriminator at the output of the processing unit (PU) based on the transformation: $L_S\xrightarrow{C\kappa}U_{\Phi\Pi}(C_\kappa,t,\tau)\to U(\mathrm{f,C_K})\to U(\hat{C}_K)\to Rang\left(U(\hat{C}_K)\right)\to Rang_i\left(\hat{C}_K\right)/_{I=1}^{\mathrm{m}}$
- determination of emergency $Rang\dfrac{ALARM}{AVAR}$ (concentration alarm condition or pre-emergency condition of the power unit by the generator power limit load).

Laser sensing of contaminated water and process liquids in combination with the optical-galvanic method of assessing the concentration of harmful substances

For comprehensive monitoring of water in the reservoirs of thermal and nuclear power plants to obtain a complete set of data on the level of chemical and dust contamination of water, it is necessary to use an integrated approach to analyze the concentration of pollutants – technological process wastes in the generation of electricity.

The integrated control method includes:

- laser sensing of liquids, gases, combustion products in gas boilers;

- use of chemical, physical and optoelectronic sensors to analyze the composition of substances;
- optical-galvanic laser control methods.

In accordance with the developed method of synthesizing a concentrator based on a laser photometer model, experimental stands for optical and galvanic studies of physical effects in technological environments, for the energy, oil and printing industries were created. To intensify data collection processes by laser sensing of samples in cuvettes, which provides a higher level of sensitivity and their chemical composition. Fig. 5 shows a diagram of the developed stand for conducting experiments on the complex optical and galvanic interaction of a laser photon beam with the substance of the sample to assess the composition of aqueous solutions and electrochemical structures.

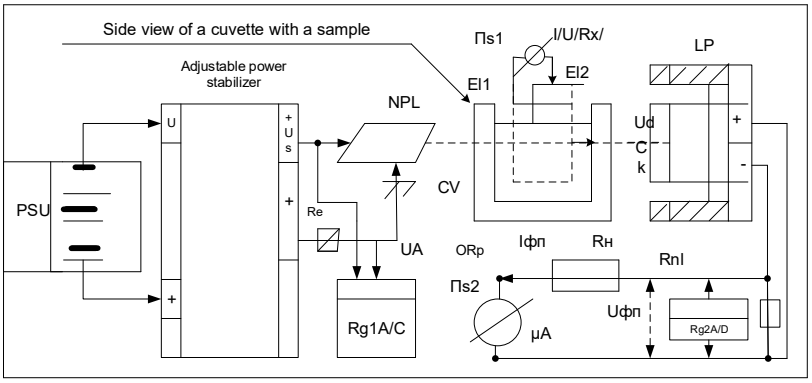


Figure 5. Stand for the study of laser effects of active interaction of substances in solutions

The block diagram includes the following units:

power supply with adjustable voltage regulator in the range $U_S \in [0-5]V$ for chang-ing the laser power;

- Rnl - load of the laser signal photodetector;
- Rd is the calibration resistance of the photoelectric signal from the matrix;
- A/C - voltage and current multimeter with a device for recording measurement data during the experiment;
- NPL - semiconductor laser with power (5, 50, 1000 mW);
- BL - geometric base of the laser and photodetector installation;
- CV - transparent cuvette with a solution of chemical components in water;
- $\{E_{li}\}$ A set of electrodes (zinc, copper, silver, carbon);
- Π_{SI} - an arrow (A/D) device for controlling the voltage (current) between electrodes E_{li} in the mode of controlling the optical-galvanic signal conversion due to quantum effects;
- PD - Photodetector of the laser signal after its passage through the cuvette with a sample of contaminated liquid and water reservoir;
- Π_{S2} a device for monitoring signals by sections of the photodetector.
- $Rg_2(A/D)$ voltage registrar at the output of the photodetector, which is generated at the moment of receiving a laser signal on the photodetector matrix and is allocated to the load resistor RU .

Models of sensors for monitoring the concentration of harmful water pollution in thermal power plant (TPP) reservoirs based on the use of optogalvanic effects

The basic model of an optical-galvanic sensor is a combination of galvanic pairs of dissimilar metal electrodes (Cu/Zn) that generate electromotive force in a liquid medium due to $\varepsilon_S = \varphi_{1(Zn)} - \varphi_{2(C_2)}$ electrode potentials (φ_1, φ_2) and activation of the liquid at the quantum level by laser photons

$$(H_2O/C\kappa) \rightarrow \left(\varphi_1 \underset{C\kappa}{\overset{KVj}{\otimes}} \varphi_2\right) \rightarrow \langle U_{1,2}(C\kappa), I_{1,2}(C\kappa)\rangle$$
$$(P_{Zl}) \rightarrow \lambda_i \rightarrow \quad \uparrow\uparrow \leftarrow (P_{Sl})/(C\kappa)$$

where: C_K - concentration of harmful emissions, (φ_1, φ_2)- potential of galvanic inter-action, Kvj - quantum photon effects of laser excitation, (P_{Zl}, P_{Sl})- power of the probing and scattered laser beam, $I_K(C_K)$- current in the galvanic couple circuit.

Let us consider the characteristics of concentration sensors using optical-galvanic effects. Here is a diagram of a measuring system for a comprehensive study of an aqueous solution and the concentration of impurities in

solutions based on the method of a comprehensive experiment on laser sensing and optical-galvanic generation of dynamic elec-tric potential to determine the level of concentration of chemicals in the products of harmful emissions during the technological process into the water environment of the TPP reservoir based on samples taken for the optical cuvette (OKp).

Based on the studies of the interaction between the laser beam energy and the aqueous medium, a signal is generated in the galvanic couple (E_{11}, E_{12}) and a laser signal is formed at the cuvette output. Based on the laser optogalvanic effect, a concentrometer scheme was developed (Fig. 6)

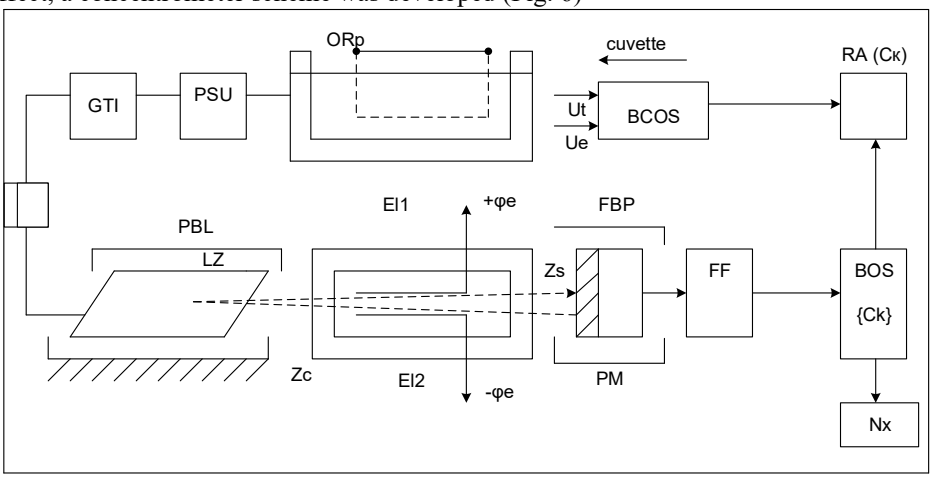


Figure 6. Schematic diagram of an optical-galvanic sensor for sampling data on the level of con-centration of impurities in water

Symbols in the diagram: PSU - power supply unit, GTI - pulse generator for laser modulation, Lz - laser for probing a sample in a cuvette, $Zc(t, Pz, fi)$ - probing laser signal with power and frequency , PBL - photo blend of laser protection, OCr - optical cuvette with a sample, (E_{l1}, E_{l2}) - electrodes of the galvanic sensor, PZ_s - signal power at the output of the cuvette, PM - photomatrix, FBP – photographic protection hood of the matrix photodetector, FF - filter unit of the laser signal after conversion in the photomatrix, BOS is a signal processing unit for estimating the level of impurity concentration in a water sample after laser sensing, - is an analog-to-digital signal converter for estimating the concentration in a discrete (digital) form of representing information about the level of water pollution, BCOS is a unit for complex processing of optical-galvanic signals from electrodes (E_{l1}, E_{l2}), RA(Ck) is an analog signal recorder from optical-galvanic and laser sensors.

The laser optical-galvanic effect when sensing samples in an optical cuvette in which the supplied water is contaminated with TPP emissions (combustion products) is the ba-sis for generating two physically different signals:

Laser sensing signal at the output of the optical cuvette (cell) of a water sample with impurities with a certain concentration level

$$(Z_G, P_C) \to R_{VS}(C_K) \otimes (P_Z, Z_S) \to \left(\alpha_S^{Ck}, P_Z\right) \to P_S(C_K)\ ,\ P_S(C_K) \xrightarrow{\alpha\Phi\Pi} U_{\Phi\Pi}(P_S(C_K)) \xrightarrow{Kus} \left\{\hat{C}_K\right\}$$

where K_{us} is the normalization factor for estimating the concentration of impurities in laser sensing.

The signal of a galvanic couple immersed in a cuvette with a water sample from a reservoir with a certain level of pollution concentration is formed according to the diagram of optical-galvanic quantum interaction during laser sensing of contaminated water samples

$$\begin{matrix}(H_2O + R(C_K)) \\ \{P_Z\}.....\end{matrix} \to \otimes \begin{matrix}\xrightarrow{E_{l1}} \\ \xrightarrow{E_{l2}}\end{matrix} Np \to \Delta U_K(P_Z, C_K, R(C_K)) \to \langle\ C_K / (\hat{\mathrm{I}}_{12}(C_K))\ \rangle\ ,$$

According to the research scheme, the variable parameters are:

- voltage, current, radiation power of a semiconductor laser due to a change in the voltage of the stabilizer, while we have

$$V_{Ar}(U_S \in [0-5]B) \to V_{Ar}(P_L \in [0 - P_{\max}])\ ,$$

- change in the concentration of impurities dissolved in the liquid in the cuvette $C_{Kd} \in [C_{K\min}, C_{K\max}]$

Taking into account the formulated methodology for assessing the level of impurity concentration, let's obtain functional characteristics:

- Concentration level $C_K \to U_{\Phi\Pi}(\mathrm{P_S}(C_K))$ at $P_L \in \{P_i - const, P_i\ \in [0-500]mBm\}$

- Photodetector output voltage as a function of concentration

$$U_{\Phi\Pi}(\mathrm{C_K}) \to \{U_{\Phi\Pi}(P_S / C_K) / P_L - const, C_{Ki} - V_{ar}\}$$

$$U_{ФП}(C_K) \rightarrow \{U_{ФП}(P_S / C_K) / P_L - V_{ar}, C_{Ki} - const\}$$
$$I_{ФП}(\mathrm{C_K}) \rightarrow \{\varepsilon_{ФП}(P_S / C_K) / P_L V_{ar}, C_K - const, R_A - const\}$$

The construction of calibration characteristics in relation to the concentration of impurities is based on

$$U - (C_K) = \psi(P_L, C_K), , I_{ФП} = \psi(R_H), U_{ФП} = \psi(R_N)$$

A low-sensitivity logarithmic scale concentrator of impurities in solution with compatible measurements is described by a system of equations that relate the level of impurity concentration to the voltage, current, potential and current of the active electrodes (Cu, Zn) for an optical galvanic sensor. $\mathrm{I_X} = I_0 \exp(-\alpha(C_K)l_K)$

$$\alpha(C_K)l_K = \ln I_x - \ln I_0 \text{ , } \alpha(C_K) = \frac{1}{l_K}\left[\ln U_{ФП}(\mathrm{P_X}) - \ln U_{ФП}(P_0)\right] \; P_{Л} = \mathrm{U_{ФП}}(I_{Л}) \cdot K_{U,P}$$

$$C_K = \psi(\alpha, V_K, l_K) \cdot \Delta U_{ФП}(\ln \mathrm{U_X} - \ln U_0)\left[\frac{мг}{см^3}\right], \mathrm{U_{ФП}} = \mathrm{I_{ФП}R_i}$$

where: C_K - concentration of impurities; α - reduced scattering coefficient; $U_{ФП}$ - photodetector voltage; $(\mathrm{V_K}, l_K)$ - volume and length of the cuvette; $Rg(A/D)$ - analog-digital data logger; ІФП - photodetector current; Ri - load resistance.

In accordance with the functional diagram, the measuring characteristics of the concentrometer (Fig. 7) are formed experimentally, taking into account the power of the prob-ing laser.

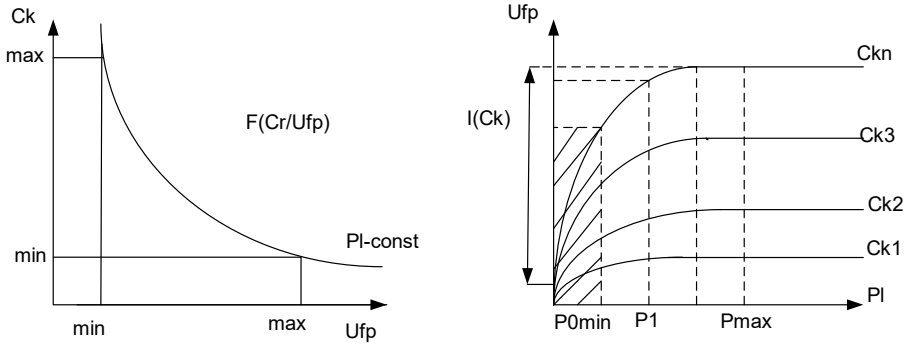


Figure 7. Characteristics of concentration measurement

The graduation characteristics of the sensors of impurity concentration in solutions and dust streams have the same model. The graduation characteristics (laser - photode-tector) are represented as a system, where $P_{л}[mBB] \in [0-500]mBB$ is the laser power; $I_{ФП}[mA] \in [0-500]mA$ photodetector current at different loads Ri.

Discussion of research results

Thus, based on the work results, we can formulate the following scientific novelty and practical significance of the research results.

The scientific novelty of the research results is the developed concept based on new information and system technologies and laser remote sensing, the method of integrated use of physical, chemical, and optical effects for the development of new type sensors, the substantiation of their information and metrological structure, synthesis methods and methods of experimental and scientific research.

Practical significance of the research results - the results of the work and analysis of global trends in the field of thermal energy, the implemented laser concentrator at Burshtyn TPP is the only project implemented in the world practice of monitoring the combustion of high-temperature fuels. Ion-selective sensors are widely used in analytical instruments and monitoring systems that are mass-produced in Ukraine and worldwide. The optical-galvanic sensors concept proposed by the authors is used to control the concentration of various impurities in the water environmental based on analytical experiments in the laboratory at the reservoir of Burshtyn TPP and other types of production, such as

1. Elevator, Rohatyn city;
2. Furniture factory in Radekhiv city;
3.Barn, village of Bibshchany;
4.Poultry farm, Hnizdychiv village.

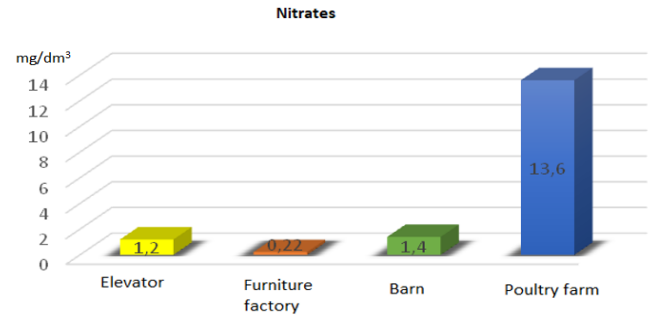


Figure 8. Chemical analysis of water from the well for 2023, the maximum concentration limit for nitrates is 50.0 mg/dm3

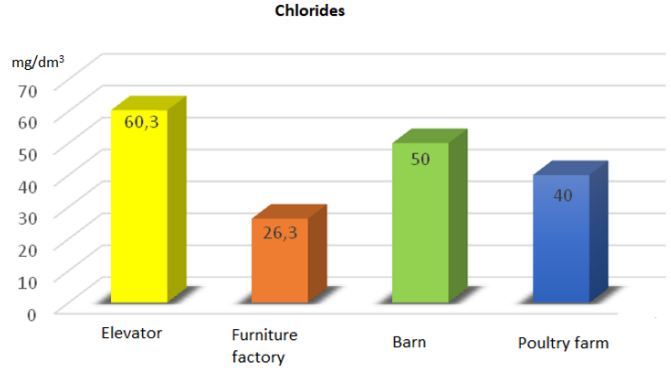


Figure 9. Chemical analysis of water from the well for 2023, the maximum concentration dose for chlorides is 300 mg/dm3

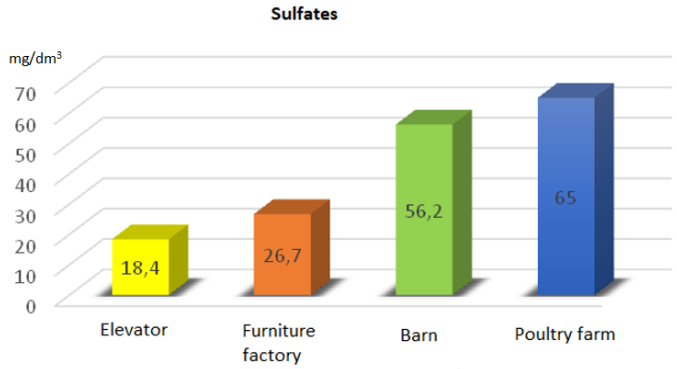


Figure 10. Chemical analysis of water from the well for 2023, the maximum concentration dose for sulfates is 500 mg/dm3

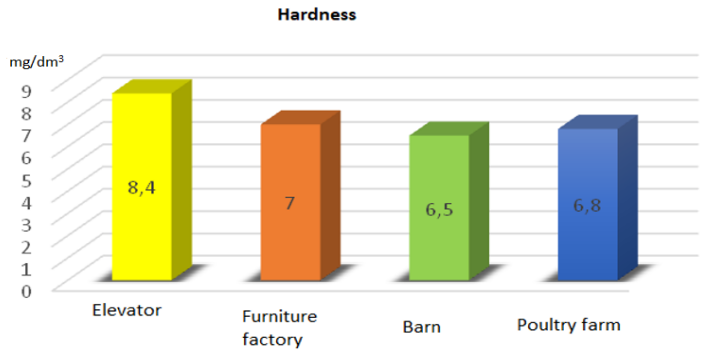


Figure 11. Chemical analysis of water from the well for 2023, the maximum concentration limit for Hardness is 7.0 mg/dm3

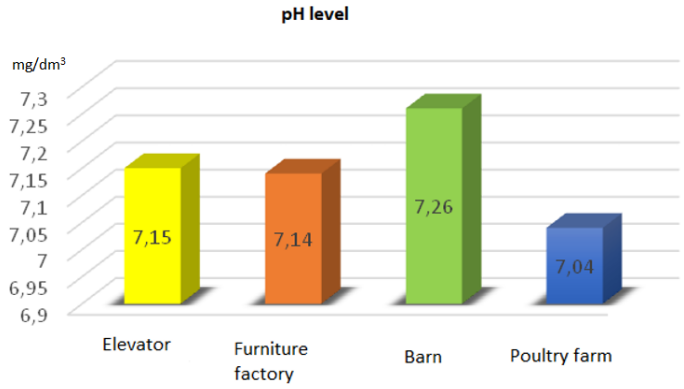


Figure 12. Chemical analysis of water from the well for 2023, the concentration limit for pH is 6.5-8.5 mg/dm3

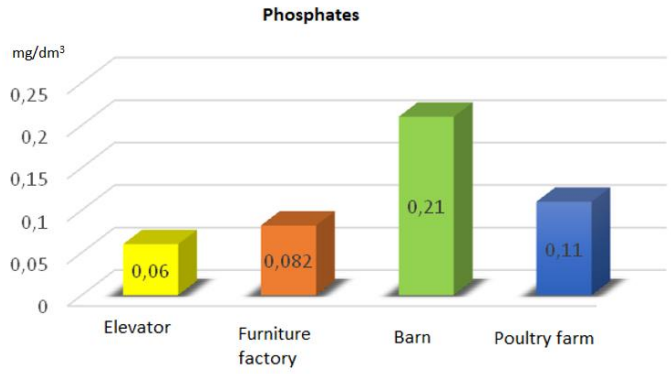


Figure 13. Chemical analysis of water from the well for 2023, the concentration limit for Phos-phate is 3.5 mg/dm3

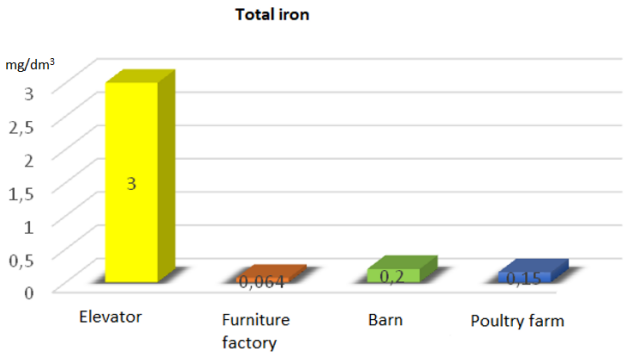


Figure 14. Chemical analysis of water from the well for 2023, the concentration limit for total iron is <1 mg/dm3

As can be seen from the graphs of water pollution from wells, we can conclude that poultry farms are the largest polluters in terms of nitrates, chlorides, and sulfates. The second place is occupied by cowsheds.

Conclusion

The article presents the theoretical foundations of creating laser sensors for measur-ing the concentration of harmful process components that enter the atmosphere and water bodies of the ecological environment of production facilities.

The article reveals the creation of information technology for the selection, processing, and classification of expert data on the state of the ecosystem of a technological facility based on the use of laser sensors to measure the concentration of harmful emissions in the air, groundwater, and water bodies.

An information model of laser sensors for measuring the concentration of harmful components in solutions and the atmosphere, which are fuel combustion products in boilers, has been developed.

The article presents elements of information technology for decision support based on the processing and classification of data from laser and optoelectronic sensors and methods for developing laser sensors for monitoring the concentration of technological hazardous waste in the atmosphere and solutions.

References

1. Jackson P., Introduction to expert systems 3rd edition, Addison-Wesley, Reading, Massachusetts, USA, 1998, 542 p.
2. Fraden J., Handbook of modern sensors: physics, designs, and applications, Springer, Berlin, Germany, 2016, 731 p.
3. Rashid M., Microelectronic circuits: analysis and design, Cengage Learning, Boston, Massachusetts, USA, 2017,912 p.
4. Deco G., Schürmann B., Information dynamics: foundations and applications, Springer, New York, 2001, 320 p.
5. Horowitz P., Hill W., The art of electronics, Cambridge University Press, New York, 2015, 1216 p.
6. Dunn P., Davis, M., Measurement and data analysis for engineering and science 4th edition, CRC Press, New York, 2017, 400 p.
7. Webster J., Eren H., Measurement, instrumentation and sensors handbook, Taylor & Francis Inc, Milton Park, Abingdon, United Kingdom, 2014, 1921 p.
8. Pries K., Quigley J., Testing complex and embedded systems, CRC Press, Boca Raton, Florida, USA, 2010, 320 p.
9. Vitovska I. V. Management activities in the field of environmental protection. Scientific and informational bulletin of the Ivano-Frankivsk University of Law named after King Danylo Halytskyi, 2023, Vol. 15 (27), pp. 135-139.
10. Boyko O., Vovna A., Zori V., Porev V., Devices and systems of environmental monitoring (Introduction to the profession), 3rd ed., DonNTU, Donetsk, Ukraine, 2013, 292 p.
11. Porter J., Arzberger P., Braun H-W., Bryant P., Gage S., Hansen T., Hanson P., Lin Ch.-Ch., Lin F.-P., Kratz T. Wireless sensor networks for ecology. BioScience, 2005, Volume 55, Issue 7, pp. 561–572.
12. Porter J.H., Nagy E., Kratz T.K., Hanson P., Collins S.L., Arzberger P. New eyes on the world: advanced sensors for ecology. BioScience, 2009, Volume 59, Issue 5, pp. 385–397.
13. Wang G., Ran G., Chen Y. and Zhang Zh. Landscape ecological risk assessment for the tarim river basin on the basis of land-use changeby. Remote Sens, 2023, Vol. 15(17), 4173.

Liubomyr Sikora **Любомир Сікора**	DrS on Engineering, Professor of Automated Control Systems Department, Institute of Computer Science and Information Technology, Lviv Polytechnic National University, Lviv, Ukraine, e-mail: lssikora@gmail.com https://orcid.org/0000-0002-7446-1980 Scopus Author ID: 24484163500	доктор технічних наук, професор кафедри автоматизованих систем управління, Інституту комп'ютерних наук та інформаційних технологій, Національного університету «Львівська політехніка», Львів, Україна.
Nataliia Lysa **Наталія Лиса**	DrS, Associate Professor of Automated Control Systems Department, Institute of Computer Science and Information Technology, Lviv Polytechnic National University, Lviv, Ukraine, e-mail: lysa.nataly@gmail.com https://orcid.org/0000-0001-5513-9614 Scopus Author ID: 36069242600	доктор технічних наук, доцент кафедри автоматизованих систем управління, Інституту комп'ютерних наук та інформаційних технологій, Національного університету «Львівська політехніка», Львів, Україна.
Olga Fedevych **Ольга Федевич**	PhD, Associate Professor of Automated Control Systems Department, Institute of Computer Science and Information Technology, Lviv Polytechnic National University, Ukraine, Lviv, Ukraine, e-mail: olha.y.fedevych@lpnu.ua https://orcid.org/0000-0002-8170-3001 Scopus Author ID: 56287826100	кандидат технічних наук, доцент кафедри кафедри автоматизованих систем управління, Інституту комп'ютерних наук та інформаційних технологій, Національного університету «Львівська політехніка», Львів, Україна.
Nazarii Khyliak **Назарій Хиляк**	PhD Student of the Department of Computer Technologies for Automation of Publishing and Printing Processes at the Institute of Printing and Media Technologies, Lviv Polytechnic National University, Ukraine, Lviv, Ukraine, e-mail: nazarii.a.khyliak@lpnu.ua https://orcid.org/0009-0000-2431-1514	аспірант кафедри автоматизації комп'ютерних технологій у видавничо-поліграфічних процесах, Інституту поліграфії та медійних технологій, Національного університету «Львівська політехніка», Львів, Україна.

https://doi.org/10.31891/csit-2025-2-7
UDC 004.912

ANDRIIV Roman
Separate structural unit "Berezhany Professional College of NUBiP of Ukraine"
SENKIVSKYY Vsevolod
Lviv Polytechnic National University

INFORMATION TECHNOLOGY FOR PREDICTING THE RELIABILITY LEVEL OF TEXT MESSAGES

The research presents the results of the creation of an intellectualized information technology for predictive analysis of the reliability of text information messages, formed on the basis of concepts and tools of fuzzy logic. The use of the fuzzy set apparatus makes it possible to take into account the semantic ambiguity inherent in a natural language, as well as to formalize qualitative expert assessments by using linguistic variables, fuzzy term-sets and a rule base of the "if-then" type. This provides the possibility of creating adaptive decision-making models in conditions of incompleteness, inconsistency and subjectivity of input information.

The developed technology includes fuzzification of input characteristics of texts, aggregation of expert judgments, construction of a system of fuzzy rules for assessing the reliability level and defuzzification of the obtained results. A concept is implemented that allows for a predictive assessment of the veracity of data even before their potential appearance in the information space. Within the framework of the proposed approach, a structured information database is formed, which establishes a relationship between the input variables, their linguistic nature, permissible ranges of values of the universal term-set, as well as clearly defined linguistic terms used for qualitative interpretation of parameters. Based on the performed structuring of linguistic variables of the studied process, a method of logical inference is developed, which represents a multi-level hierarchy of relationships between database components and determines the algorithm for calculating the message reliability indicator. The method is based on a knowledge matrix, leading to the construction of fuzzy logical equations, which provide the calculation of normalized values of membership functions of linguistic variables at the division points of the universal set. The result is the defuzzification of the fuzzy set "the indicator of the reliability level of text information messages" and the calculation of its value using the centre of mass formula, taking into account the input data. As a result of the study, a structural model of the information technology component of assessing the veracity of news content is developed.

Keywords: reliability of text messages, linguistic variable, logical inference method, knowledge matrix, membership function, fuzzy logic equations, information technology.

АНДРІЇВ Роман
Відокремлений структурний підрозділ «Бережанський фаховий коледж НУБіП України»
СЕНЬКІВСЬКИЙ Всеволод
Національний університет «Львівська політехніка»

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПРОГНОЗУВАННЯ РІВНЯ ДОСТОВІРНОСТІ ТЕКСТОВИХ ПОВІДОМЛЕНЬ

У межах дослідження представлено результати створення інформаційної технології прогнозного аналізу достовірності текстових інформаційних повідомлень, побудованої на основі концепцій і засобів нечіткої логіки. Застосування апарату нечітких множин дало змогу враховувати семантичну неоднозначність, притаманну природній мові, а також формалізувати якісні експертні оцінки шляхом використання лінгвістичних змінних, нечітких терм-множин і бази правил типу «якщо-то». Це забезпечує можливість побудови адаптивних моделей прийняття рішень в умовах неповноти, суперечливості та суб'єктивності вхідної інформації.

Розроблена технологія включає фазифікацію вхідних характеристик текстів, агрегування експертних суджень, побудову системи нечітких правил для оцінювання рівня достовірності та дефазифікацію отриманих результатів. Реалізовано концепцію, яка дозволяє здійснювати прогнозну оцінку правдивості даних ще до їх потенційної появи в інформаційному просторі. У межах запропонованого підходу сформовано структуровану інформаційну базу даних, яка встановлює зв'язок між вхідними змінними, їхньою лінгвістичною природою, допустимими діапазонами значень універсальної терм-множини, а також чітко визначеними лінгвістичними термами, що застосовуються для якісної інтерпретації параметрів. На основі виконаного структурування лінгвістичних змінних досліджуваного процесу розроблено метод логічного виведення, що відтворює багаторівневу ієрархію зв'язків між компонентами бази даних та визначає алгоритм розрахунку показника достовірності повідомлень. В основі методу лежить матриця знань, що обумовила побудову нечітких логічних рівнянь, які забезпечили розрахунок нормалізованих значень функцій належності лінгвістичних змінних у точках розподілу універсальної множини. Наслідком стала дефазифікація нечіткої множини «показник рівня достовірності текстових інформаційних повідомлень» та розрахунок за формулою центра мас його значення з урахуванням введених вхідних даних. У підсумку дослідження розроблено структурну модель компоненти інформаційної технології оцінювання правдивості новинного контенту.

Ключові слова: достовірність текстових повідомлень, лінгвістична змінна, метод логічного виведення, матриця знань, функція належності, нечіткі логічні рівняння, інформаційна технологія.

Introduction

In the modern information environment, the problem of assessing the reliability of text messages is becoming particularly relevant due to the high level of information noise, the spread of manipulative content and fake messages. The process of determining the reliability level is characterized by a significant number of subjective

factors that are difficult to formalize by traditional methods. In this context, there is a need to develop flexible and adaptive solutions that can take into account the uncertainty and ambiguity inherent in a natural language.

For this purpose, the study proposes an information technology for predictive assessment of the reliability of text information messages, based on the use of fuzzy logic. This approach allows one to model linguistic variables, formalize expert judgments and implement the decision-making process in conditions of vaguely defined input parameters. The proposed technology is universal in the sense that it can be adapted to various thematic domains, types of information and sources, which provides wide possibilities for practical application – from automated monitoring of news streams to assessing the reliability in social networks.

An important component of the study is a review of publications related to the declared topic, which will determine the relevance and reliability of the results obtained.

The development of automated fake news detection methods is a key area of modern research in the field of information security. The works [1–4] present a wide range of approaches, covering probabilistic models, structural text analysis, graph convolutional networks and intelligent frameworks for data analysis in social networks. These solutions are aimed at identifying unreliable information using formalized characteristics that indicate potential distortion of facts or manipulativeness. Algorithmic methods, in particular machine learning, are increasingly used as an alternative to traditional manual fact-checking [5], but remain dependent on the quality and completeness of training samples. In this context, there is growing interest in models that take into account not only the content, but also the behavioural aspects of users of the information environment [6], and are also aimed at developing the digital literacy of future media professionals [7]. Of particular scientific value are approaches that integrate fuzzy logic tools into the process of automated message reliability analysis [8–9]. Such solutions allow creating adaptive systems that can work effectively in conditions of incomplete or fuzzy data, in particular in library information environments. The use of hybrid models that combine fuzzy logic with deep learning methods significantly improves the accuracy and reliability of fake news detection [9], especially in conditions of increased sensitivity to data security, for example, in IoT environments [10]. In this case, decision-making algorithms based on extended fuzzy logical inference are implemented, which takes into account the complexity and dynamics of information flows. The works [11–12] substantiate the advantages of using intelligent control systems using fuzzy logic to increase the reliability of decision-making in complex information environments. By using membership functions and fuzzy rules, such systems are able to effectively respond to multifactorial influences and ensure stability in situations of information uncertainty. Fake news is increasingly being considered as a tool for targeted disinformation activities [13], which requires a comprehensive analysis taking into account both technical and social factors of content distribution. For a wide range of users, it is advisable to apply reliability assessment criteria that do not require special training, but allow one to recognize signs of unreliability, in particular emotionality, sensationalism and lack of accuracy [14]. In the media analytical context, a balance between facts and value judgments is important, which ensures the completeness and objectivity of the information presented [15].

The analysis of scientific sources allows one to conclude that despite the significant number of modern approaches to detecting fake news, the application of the reliability fuzzy logic apparatus remains limited. In this regard, it is urgent to create unified information models and information technologies based on the fuzzy set theory, which will provide a predictive assessment of the reliability of information messages.

Formation of an indicator for assessing the reliability of text information messages

Taking into consideration the complexity and multi-factor nature of the process of assessing the reliability of text information messages, this study substantiates, as noted above, the feasibility of using the fuzzy logic apparatus. Within the framework of the study, a structured information database is formed that establishes the relationship between input variables, their linguistic nature, permissible ranges of values of the universal term-set, as well as clearly defined linguistic terms used for qualitative interpretation of parameters.

The linguistic variable of the reliability of text messages is presented as a function:

$$Q = F_Q\left(B,T,L\right), \tag{1}$$

the arguments of which are linguistic variables (LV) of the second level B,T,L. At this level, the linguistic variable B is oriented towards factors of organizational orientation (b_1 – a source of information, b_2 – fact checking, b_3 – multiple publication); T defines a procedure-function related to the author and the context of the message (t_1 – professionalism of the author, t_2 – objectivity of the author, t_3 – informativeness of the message context); L characterizes the share of the indicator assessed by the attitude of users towards the received news (l_1 – refutation and criticism, l_2 – social trust)

Let one form a table of term-sets of linguistic variables, including the description of LV and a database of values [17].

Table 1

Term-sets of values of linguistic variable

LV	Linguistic description of the variable	Universal base of values U	Linguistic terms (term-set H)
b_1	A source of information (reliability)	(1-5) c. u.	Low, medium, high
b_2	Fact checking	(1-5) c. u.	Infrequent, frequent, constant
b_3	Multiple publication (quantity)	(1-5) c. u.	Small, medium, large
t_1	Professionalism of the author	(1-5) c. u.	Low, medium, high
t_2	Objectivity of the author	(1-5) c. u.	Low, medium, high
t_3	Informativeness of the message context	(1-5) c. u.	Low, medium, high
l_1	Refutation and criticism (frequency)	(1-5) c. u.	Small, medium, significant
l_2	Social trust	(1-5) c. u.	Low, medium, high

Based on the structuring of linguistic variables in the predictive assessment process of the reliability of text information messages, a method of logical inference is developed that reproduces a multi-level hierarchy of relationships between database components and determines the algorithm for calculating the RTIM indicator.

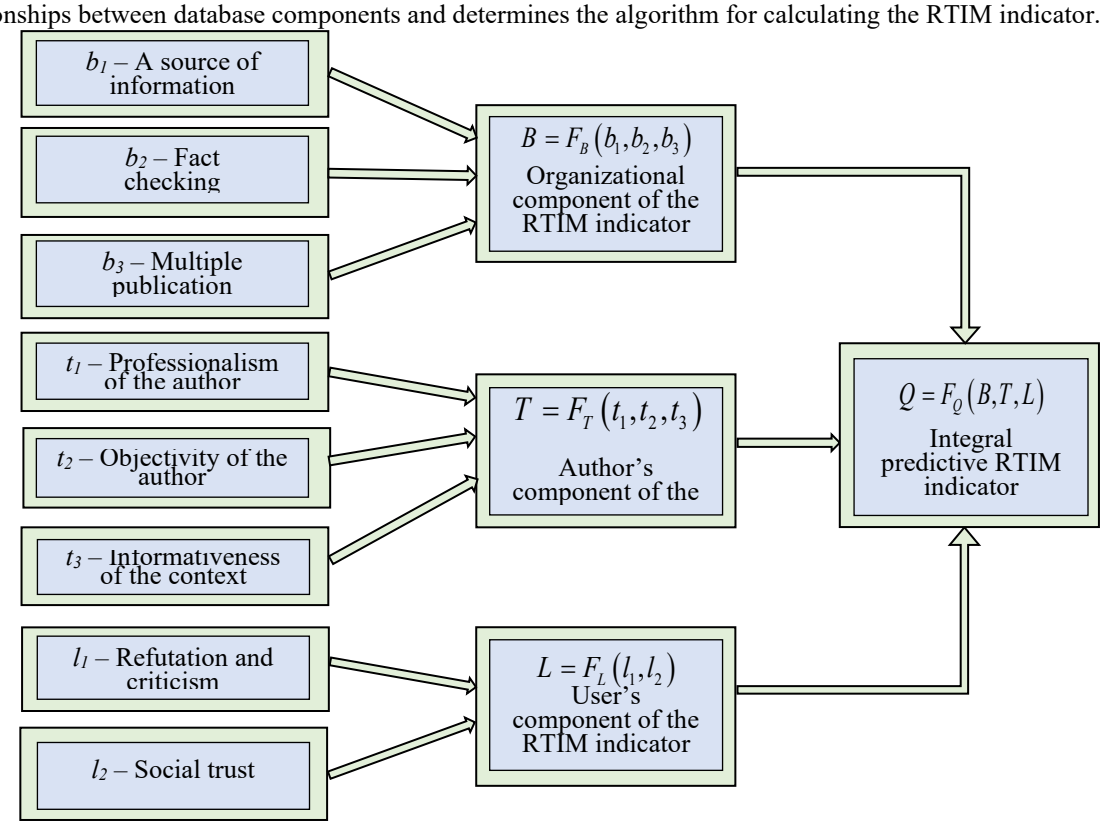


Fig. 1. Structural model of the logical inference method – formation of the indicator of the reliability of text information messages

Taking into account the above, the linguistic term "the indicator of reliability of text messages" is displayed as a fuzzy set [16]:

$$Q = \left\{ \frac{\mu_q(u_1)}{u_1}, \frac{\mu_q(u_2)}{u_2}, ..., \frac{\mu_q(u_n)}{u_n} \right\}, \tag{2}$$

where: $Q \subset U$; $\mu_q(u_i)$ is a membership function (MF) of the element $u_i \in U$ to the set Q .

For each LV and its corresponding three linguistic term-sets $_H$, square inversely symmetric matrices $A = a_{ij}$ ($a_{ij} = r_i / r_j$; $i, j = 1,...,5$) are constructed, the elements of which are formed by comparing ranks with each other. Fuzzy logical inference for the highest level has the following formalized form [17]:

IF (B = low) AND (B = medium) AND (B = high)
AND (T = low) AND (T = medium) AND (T = high)
AND (L = low) AND (L = medium) AND (L = high),
THEN (Q = low) AND (Q = medium) AND (Q = high).

The formulated logical inference determines the development of the corresponding knowledge matrix in the form of Table 2.

Table 2

Knowledge matrix for the linguistic variable Q

Organizational component of RTIM B	Author's component of RTIM T	User's component of RTIM L	Integral RTIM indicator Q
low	low	low	low
low	medium	low	
medium	low	medium	medium
medium	medium	high	
high	high	medium	high
high	high	high	

Based on the knowledge matrix in Table 2, fuzzy logical equations are constructed that provide the calculation of the values of membership functions.

$$\mu_{low}(Q) = \mu_{low}(B) \wedge \mu_{low}(T) \wedge \mu_{low}(L) \vee \mu_{low}(B) \wedge \mu_{low}(T) \wedge \mu_{low}(L).$$

$$\mu_{medium}(Q) = \mu_{medium}(B) \wedge \mu_{low}(T) \wedge \mu_{medium}(L) \vee \mu_{medium}(B) \wedge \mu_{medium}(T) \wedge \mu_{high}(L).$$

$$\mu_{high}(Q) = \mu_{high}(B) \wedge \mu_{high}(T) \wedge \mu_{середня}(L) \vee \mu_{high}(B) \wedge \mu_{high}(T) \wedge \mu_{high}(L).$$

The specified approach is applied to LV of the following levels B, T and L.

The linguistic term Q "the indicator of reliability of text information messages" is presented in the form of a fuzzy set [16]:

$$Q(B,T,L) = \left\{ \frac{\mu_{low}(Q)}{q_1}, \frac{\mu_{medium}(Q)}{q_2}, \frac{\mu_{high}(Q)}{q_3} \right\}, \quad (3)$$

where q_1, q_2, q_3 determine the quantitative values of the linguistic variable Q in relation to the above-mentioned terms at the division points of the universal set.

Experiments

At the final stage of theoretical research, after determining the main linguistic variables and constructing the corresponding membership functions, these variables are formalized in the form of table structures. For this purpose, tables with normalized values of membership functions at five characteristic division points of the universal set are formed for each of the selected linguistic variables. This approach allows ensuring the consistency and correctness of further calculations within the fuzzy logic system.

An example of constructing the corresponding table for a linguistic variable is presented below, which at the same time serves as the basis for moving to the experimental stage of research, where the constructed model is tested on the basis of real or simulated input data.

Table 3

Membership functions of the term-set $H(b_1)$ (a source of information – reliability)

u_i, c. U.	1	2	3	4	5
$\mu_{low}(u_i)$	1	0,86	0,54	0,34	0,11
$\mu_{medium}(u_i)$	0,12	0,66	1	0,56	0,12
$\mu_{high}(u_i)$	0,11	0,33	0,56	0,78	1

The next step is to select the points of the universal set U and their corresponding values of the membership functions. Let the following input data be selected for the linguistic variables:

$$b_1 = 5;\ b_2 = 3;\ b_3 = 4;\ t_1 = 4;\ t_2 = 3;\ t_3 = 2;\ l_1 = 3;\ l_2 = 4$$

and their corresponding values of the membership functions.

By substituting the given values into fuzzy logical equations, the values of the membership functions for linguistic variables B, T, L are obtained:

$$\mu_{low}(B) = 0{,}11;\ \mu_{medium}(B) = 0{,}12;\ \mu_{high}(B) = 0{,}40;$$
$$\mu_{low}(T) = 0{,}30;\ \mu_{medium}(T) = 0{,}50;\ \mu_{high}(T) = 0{,}12;$$
$$\mu_{low}(L) = 0{,}22;\ \mu_{medium}(L) = 0{,}30;\ \mu_{high}(L) = 0{,}50.$$

The membership functions of the highest-level linguistic variable are calculated:

$$\mu_{low}(Q) = 0{,}11;\ \mu_{medium}(Q) = 0{,}12;\ \mu_{high}(Q) = 0{,}12.$$

The process of determining the quantitative indicator of the reliability level of text information messages is implemented by using the centre of mass method, which is one of the most common defuzzification methods within fuzzy logic. This method allows one to move from linguistic assessments, presented in the form of fuzzy sets, to a specific numerical value that characterizes the predictive level of information reliability.

The indicator of predictive reliability of information messages P is calculated using the following formula [17]:

$$P = \frac{\sum_{i=1}^{m}\left[\underline{Q} + (i-1)\frac{\overline{Q} - \underline{Q}}{m-1}\right]\mu_i(Q)}{\sum_{i=1}^{m}\mu_i(Q)}, \quad (9)$$

where: $\underline{Q}, \overline{Q}$ mean the minimum and maximum values of the message reliability indicator; m is a number of fuzzy terms of the linguistic variable Q. For calculations, the following initial values are set: $m = 3$; $\mu_1(Q) = \mu_{low}(Q)$, $\mu_2(Q) = \mu_{medium}(Q)$, $\mu_3(Q) = \mu_{high}(Q)$. Lower and upper limits of values for the linguistic variable Q are presented as a percentage: $\underline{Q} = 1\%$; $\overline{Q} = 100\%$.

The calculations are performed at three points of the specified interval: $q_1 = 1$; $q_2 = 50$; $q_3 = 100$. Finally, according to formula (9), the following value of the message reliability level indicator is obtained: $P = 51{,}74\%$. The indicator calculated at the given input values of linguistic variables indicates the *average* reliability level of the information message.

Taking into account the theoretical and experimental components of the study, a key component of information technology will be designed for predictive assessment of text message reliability.

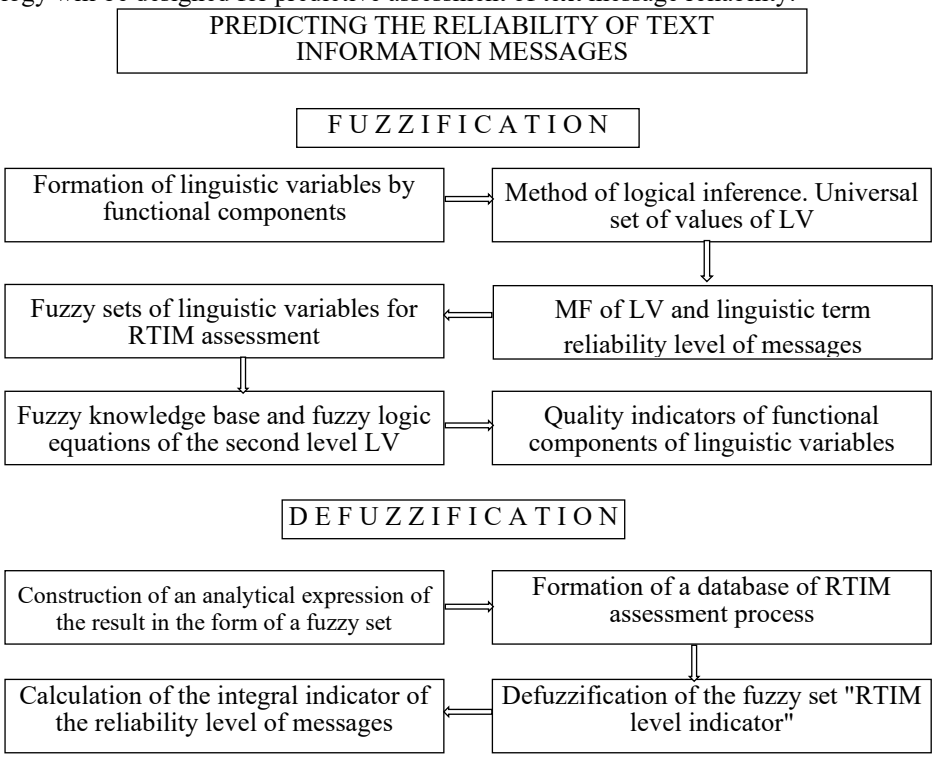


Fig. 2. Structural model of the information technology component of predictive assessment of the text message reliability

The developed structural model of the key component of the information technology for predictive assessment of the text message reliability provides a holistic view of the interaction of the main subsystems focused on processing, analysis and interpretation of text data, taking into account multi-factor influence. The central element of the model is the method of fuzzy logical inference, which integrates the results of preliminary linguistic and semantic processing, reliability parameters, as well as contextual characteristics of messages. The architecture of the model provides for adaptive tuning based on expert knowledge, weight coefficients of influence factors and membership functions, which allows forming a generalized indicator of the reliability level, taking into account incompleteness, inconsistency or unstructuredness of information. The model can be effectively integrated into application systems for monitoring the information environment, increasing the accuracy of detecting fake news and contributing to making informed decisions in the field of information security.

Conclusions

As a result of the research, a key component of intellectualized information technology for predictive assessment of the reliability of text messages, based on fuzzy logic tools, is developed. The proposed approach allows to effectively formalize subjective expert judgments and adapt the analysis process to the conditions of semantic uncertainty characteristic of a natural language. The basis of the implemented technology is a system of fuzzification, aggregation, logical inference and defuzzification, which provides multi-level processing of text information taking into account linguistic variables and their values in the term-space.

An information database is designed that establishes relationships between input parameters, their linguistic representation and permissible ranges of values. A method of fuzzy logical inference is developed, which is based on a knowledge matrix and a hierarchy of the process of forming a message reliability indicator and allows calculating the reliability level using a system of logical equations. The target indicator value is determined using the center of mass method, which provides an integrated quantitative assessment of the message reliability.

As a result, a structural model of a key component of information technology is formed, which can be used to assess the veracity of news content at the stage of its appearance or distribution in the information space, which opens up prospects for its integration into information monitoring systems and countering disinformation. This approach allows not only to carry out multifactor analysis of messages, but also to effectively generalize assessments from different sources. The proposed technology is characterized by a high degree of versatility, since its architecture allows the adaptation to different subject areas, genre features of texts and the specificity of information sources. This creates broad prerequisites for practical implementation – in particular, in the tasks of automated monitoring of news flows, verification of information in social media, as well as in the field of information security.

References

1. D. K. Dixit, A. Bhagat and D. Dangi. Automating fake news detection using PPCA and levy flight-based LSTM. Soft Comput., num. 26, num. 22 (2022) 12545–12557. https://doi.org/10.1007/s00500-022-07215-4.
2. Y. Wang, L. Wang, Y. Yang and Y. Zhang. Detecting fake news by enhanced text representation with multi-EDU-structure awareness. Expert Syst. Appl., num. 206 (2022). https://doi.org/10.1016/j.eswa.2022.117781.
3. D. Michail, N. Kanakaris and I. Varlamis. Detection of fake news campaigns using graph convolutional networks. Int. J. Inf. Manag. Data Insights, num. 2 (2022). https://doi.org/10.1016/j.jjimei.2022.100104.
4. S. Rastogi, D. Bansal. Disinformation detection on social media: An integrated approach. Multimed. Tools Appl., num. 81, num. 28 (2022) 40675–40707. https://doi.org/10.1007/s11042-022-13129-y.
5. Rastogi, S., Bansal, D. A review on fake news detection 3T's: typology, time of detection, taxonomies. Int. J. Inf. Secur. 22 (2023) 177–212. https://doi.org/10.1007/s10207-022-00625-3.
6. Ines Kožuh, Peter Čakš Social Media Fact-Checking: The Effects of News Literacy and News Trust on the Intent to Verify Health-Related Information October Healthcare, (2023) 11(20):2796 DOI: 10.3390/healthcare11202796.
7. Lyudmila Shesterkina, Lidiya Lobodenko, Anna Krasavina, Arina Marfitsyna Fact-Checking and Information Verification in the Context of Journalism Education (March 2021). Theoretical and Practical Issues of Journalism 10(1):94-108 DOI: 10.17150/2308-6203.2021.10(1).
8. Nikolaou, N., & Karypis, G. Automated fake news detection: A survey. Social Network Analysis and Mining, 10(1) (2020) 1-29. DOI: 10.6017/ital.v39i4.12483.
9. Cheng Xu and M-Tahar Kechadi. 2023. Fuzzy Deep Hybrid Network for Fake News Detection. In The 12th International Symposium on Information and Communication Technology (SOICT 2023), December 07–08 (2023), Ho Chi Minh, Vietnam. ACM, New York, NY, USA 8 Pages. https://doi.org/10.1145/3628797.3628971.
10. Memon, I., Shaikh, R. A., Hasan, M. K., Hassan, R., Haq, A. U., & Zainol, K. A. (2020). Protect mobile travelers information in sensitive region based on fuzzy logic in IoT technology. Security and Communication Networks, (1), (2020) 8897098. DOI:10.1155/2020/8897098.
11. Dumitrescu, C., Ciotirnae, P., & Vizitiu, C. Fuzzy logic for intelligent control system using soft computing applications. Sensors, 21(8), (2021) 2617. https://doi.org/10.3390/s21082617.
12. Daradkeh, Y. I., & Tvoroshenko, I. Technologies for making reliable decisions on a variety of effective factors using fuzzy logic. International Journal of Advanced Computer Science and Applications, 11(5), (2020). DOI: 10.14569/IJACSA.2020.0110507.
13. NORDBERG, Pontus; KÄVRESTAD, Joakim; NOHLBERG, Marcus. Automatic detection of fake news. In: 6th International Workshop on Socio-Technical Perspective in IS Development, virtual conference in Grenoble, France, June 8-9, 2020. CEUR-WS, (2020). p. 168-179.
14. Z. Brzhevska, H. Haydur, N. Dovzhenko, A. Anosov. Criteria for monitoring the reliability of information in the information space. Cyber security: education, science, technology, No. 1(5), 2019, pp. 105-112. (2019). https://doi.org/10.28925/2663-4023.5.52.60.

15. Marcheniuk, M. S., Kozachok, V. A., Bogdanov, O. M., Brzhevska, Z. M. Analysis of methods of detecting disinformation in social networks using machine learning. Cyber security: education, science, technology, No. 2(22) (2023). pp. 148-155. https://doi.org/10.28925/2663- 4023.2023.22.148155.
16. B. V. Durnyak, I. V. Pikh, V. M. Senkivskyi. (2022). Theoretical foundations of the information concept of forming and assessing the quality of publishing and printing processes. Monograph. – Lviv: Ukrainian Academy of Printing. 356 p. URL: https://biblio.uad.lviv.ua.
17. Vsevolod Senkivskyy, Iryna Pikh, Alona Kudriashova, Roman Andriiv, Nazarii Senkivskyi. Evaluation of methods for intellectual analysis of manipulative content in the information space. The 6th International Workshop on Intelligent Information Technologies & Systems of Information Security, 2025, Khmelnytskyi, Ukraine. Pp. 139-155. https://ceur-ws.org/Vol-3963/paper12.pdf

Roman Andriiv **Роман Андріїв**	Teacher of mathematics, physics and computer science of the cyclical commission of physical and mathematical disciplines and information technologies Separate structural unit «Berezhany Professional College of NUBiP of Ukraine» Berezhany, Ternopil region, Ukraine e-mail: roman.andriiv@icloud.com https://orcid.org/0009-0001-2450-5439 Scopus Author ID: 59548768000	Викладач математики, фізики та інформатики циклової комісії фізико-математичних дисциплін та інформаційних технологій Відокремлений структурний підрозділ «Бережанський фаховий коледж НУБіП України», Тернопільська обл., Україна
Vsevolod Senkivskyy **Всеволод Сеньківський**	Doctor of Technical Sciences, Professor, Professor of Computer Technologies in Publishing and Printing Processes Department, Lviv Polytechnic National University, Lviv, Ukraine, e-mail: vsevolod.m.senkivskyi@lpnu.ua https://orcid.org/0000-0002-4510-540X Scopus Author ID: 57208667450	Доктор технічних наук, професор, професор кафедри комп'ютерних технологій у видавничо-поліграфічних процесах, Національний університет «Львівська політехніка», Львів, Україна.

https://doi.org/10.31891/csit-2025-2-8
UDC 004.67: 612.113

CHUIKO Gennady, YAREMCHUK Olga
Petro Mohyla Black Sea National University, Mykolaiv, Ukraine

COMPUTERISED BLOOD PRESSURE MONITORING IN OUTPATIENT SETTINGS

The paper presents the measurement of a normal 24-hour heart rate and blood pressure analysis of an anonymous patient. The object of study in this paper is the computer processing of outpatient blood pressure monitoring. The goal is to mathematically model the data as a sum of relatively smooth trends and detrended fluctuations. Tasks: decomposition of the primary series by two independent methods, stability and spectral analysis of the shifted fluctuations using the Wiener-Hinchin theorem, and proving the self-similarity of such fluctuations. The methods used are: singular spectrum analysis, exponential smoothing of the simulation, and analysis of autocorrelation functions. The following results are obtained. The dataset is a sum of relatively smooth trends and detrended fluctuations; blood pressure trends have certain nighttime minima; detrended fluctuations are fractional Gaussian noise with a Hurst index of about (0.80 ± 0.016), the energy spectra of detrended fluctuations were found for the first time. Scientific novelty of the results: 1) the measured 24-hour heart rate and blood pressure analyses are decomposed into relatively smooth trends and detrended fluctuations; 2) trends allow for a more reliable assessment of 24-hour, nightly and daily average blood pressure values, which are the leading indicators of a series of blood pressure measurements and monitoring; 3) detrended fluctuations contain other valuable diagnostic information, such as short-term blood pressure variability or persistence index. 4) fluctuation analysis provides information about the power spectra of the blood pressure monitoring series and their similarity to the spectra of fractional Gaussian noise; 4) knowledge of short-term changes in blood pressure is the basis for constructing informative repeatability graphs for blood pressure monitoring; 5) detrended fluctuations are identified as fractional Gaussian noise, which is a self-similar stochastic process.

Keywords: mathematical modelling, computing technologies, singular spectrum analysis, fluctuation analysis, stochastic process, computer blood pressure monitoring.

ЧУЙКО Геннадій, ЯРЕМЧУК Ольга
Чорноморський національний університет імені Петра Могили, Миколаїв, Україна

КОМП'ЮТЕРНИЙ МОНІТОРИНГ АРТЕРІАЛЬНОГО ТИСКУ В АМБУЛАТОРНИХ УМОВАХ

В роботі представлено вимірювання звичайного 24-годинного пульсу і аналіз артеріального тиску анонімного пацієнта. Об'єктом вивчення в статті є комп'ютерна обробка амбулаторного моніторингу артеріального тиску. Метою є математичне моделювання даних, як сума відносно плавних трендів і детрендованих флуктуацій. Завдання: розкладання первинного ряду двома незалежними методами, стійкість та спектральний аналіз зміщених флуктуацій, використовуючи теорему Вінера-Хінчина та доведення самоподібності таких флуктуацій. Використовуваними методами є: сингулярний аналіз спектру, експоненціальне згладжування моделювання та аналіз автокореляційних функцій. Отримані такі результати. Набір даних являє собою суму досить плавних трендів і детрендованих флуктуацій; тренди артеріального тиску мають певні нічні мінімуми; детрендовані флуктуації - це дробові гаусові шуми з показником Херста близько (0.80 ± 0.016), енергетичні спектри детрендованих флуктуацій були знайдені вперше. Наукова новизна отриманих результатів: 1) виміряний 24-годинний пульс і аналізи артеріального тиску розкладаються на досить плавні тренди і детрендовані флуктуації; 2) тренди дозволяють більш надійно оцінювати 24-годинні, нічні та добові середні значення артеріального тиску, які є головними індикаторами серії вимірювання та моніторингу артеріального тиску; 3) детрендовані коливання містять іншу цінну діагностичну інформацію, таку як короткочасна варіабельність артеріального тиску або показник персистенції. 4) флуктуаційний аналіз надає інформацію про спектри потужності серії моніторингу артеріального тиску та їх подібність до спектрів часткового шуму Гауса; 4) знання короткочасових змін артеріального тиску є основою для побудови інформативних графіків повторюваності для моніторингу артеріального тиску; 5) детрендовані флуктуації ідентифікуються як фракційний гаусовий шум, який є самоподібним стохастичним процесом.

Ключові слова: математичне моделювання, технології виконання обчислень, сингулярний аналіз спектру, флуктуаційний аналіз, стохастичний процес, комп'ютерний моніторинг артеріального тиску.

Introduction

Ambulatory blood pressure monitoring (ABPM) is a widely recognized technique for diagnosing hypertension. From a clinical perspective, the most valuable information is the 24-hour average and nocturnal blood pressure readings. Other derived indices of ABPM also have clinical significance, albeit to a lesser extent [1]. Routine ABPM involves a few dozen trials over 24 hours that are more or less regular, often averaged within each hour [2]. This ordinary and cheap test solves a pretty lengthy and impressive list of diagnostic problems [3]:

1) Identify "white coat" hypertension.
2) Identify masked hypertension.
3) Detect standard 24-hour blood pressure patterns (dipping, daytime, and nocturnal hypertension).
4) Assess hypertension treatment.
5) assessing hypertension in the elderly, children/adolescents, pregnancy, and high-risk patients.
6) Identify ambulatory hypotension.
7) Identify blood pressure patterns in Parkinson's Disease.
8) endocrine Hypertension.

The authors [4] presented statistical data from five prominent medical centers known for their work in ambulatory blood pressure monitoring (ABPM). This data indicates a trend in the increasing use of ABPM, suggesting that its growth is primarily due to its clinical benefits rather than reimbursement incentives. The statistics show a steady rise in ABPM testing over time.

The use of ABPM to monitor treatment can be notably facilitated by software capable of providing a trend report [4]. Although the adverse cardiovascular consequences of hypertension primarily depend on average blood pressure values [1], evidence from observational studies and clinical trials has shown that these outcomes may also depend on increased short-term and long-term blood pressure variability (see [5] and [6]).

Trend analysis in ABPM helps identify long-term blood pressure patterns, including sustained hypertension and nocturnal dipping patterns. Such information is crucial for diagnosing conditions like nocturnal hypertension, which often go unnoticed in clinical settings [7].

Detrended fluctuation analysis (DFA) is increasingly being explored in ABPM to reveal subtle, long-range correlations in blood pressure variability, particularly those associated with cardiovascular risk and autonomic regulation [8]. However, recent studies specifically applying DFA to ABPM remain relatively niche. The contribution of our research may be defined as an extention og this niche.

Related works

It is reasonable to break down ABPM readings into at least two components: smooth trends and pure fluctuations free of trends. The first component reflects low-frequency signals, which indicate averaged parameters. The second component relates to high-frequency signals associated with short-term variability. We are only referring to short-term variability, as there are valid concerns about whether long-term variability can be accurately determined from standard ABPM readings [5,7].

Research has also been conducted on the multifractal multiscale analysis of detrended fluctuations using the DFA method [8,9]. The goal is to enhance clinical procedures for more accurate cardiovascular risk assessment. Additionally, this research could aid in analyzing day/night variations in blood pressure. The application of real-time heart rate variability as a predictor of hemodialysis efficiency in patients with end-stage kidney disease is detailed in [10].

However, attempts to decompose ABPM data are still relatively rare [7, 8, 11, 12]. The issue arises because commonly used digital filters, such as wavelets, typically involve two-fold downsampling, which is undesirable for short series like those in ABPM [12]. Meanwhile, innovative methods, such as ABPM registration using computer vision techniques [13], enable continuous blood pressure monitoring, allowing data series to be as lengthy and detailed as needed. Nevertheless, traditional ABPM methods will continue to produce short series.

It is essential to note that methods are available that do not require downsampling of short time series. For instance, Principal Component Analysis (PCA) is closely related to the Poincaré Plot technique, especially when considering these plots for embedding short ABPM series in a two-dimensional space [12, 14].

Another method, Singular Spectrum Analysis (SSA), is often considered more suitable for more extended series [15]. However, its effectiveness for short series should also be evaluated. A third method that might be utilized is Exponential Smoothing Modeling (ESM) [16, 17], which involves decomposing the studied series. An attempt to apply ESM to DFA can be found in [18]. Nonetheless, the authors are not aware of any examples of the ESM technique utilizing ABPM data, which inspired us.

Aim and tasks

Express-analyze of publications hints at two principal different, but mutually ancillary, approaches to ABPM:

1. Usage of advanced but more expensive registration techniques ([13])
2. Usage of advanced but more complex processing methods ([11] and [12])

Based on the abovementioned point, one can formulate the article's primary purpose. The aim is to predict the reliable separation of the ABPM series on smooth trends and fluctuations, free of trends (detrended ones), for deeper insight into the ABPM structure and more reliable diagnostics.

Trends shall reflect the average features of the ABPM series, including nocturnal dipping. At the same time, the detrended fluctuation analysis (DFA) will inform us about the series' persistence and self-similarity if they exist.

The following tasks were formulated to achieve the stated goal:

a) Data Decomposition: Divide the ABPM time series into smooth trends and detrended fluctuations using SSA and ESM. Compare and validate the results obtained from these two independent methods.

b) Persistence Analysis: Perform Detrended Fluctuation Analysis (DFA) to evaluate the persistence and self-similarity of the detrended fluctuations. Estimate the Hurst exponent to quantify the memory effect in blood pressure variability.

c) Variability Characterization: Apply Principal Component Analysis (PCA) to quantify short-term variability in ABPM data. Construct recurrence plots to visualize and analyze patterns within detrended fluctuations, including their recurrence ratios and entropy.

d) Clinical Relevance Assessment: Analyze trends to determine 24-hour, nocturnal, and diurnal average blood pressure values. Assess the significance of nocturnal dipping and identify diagnostic indicators derived from trends and fluctuations in blood pressure.

Theory and Experiments Origin and Brief Description of Data

CardiacDirect (https://www.cardiacdirect.com/) is a US-based medical equipment supplier specializing in cardiac devices and accessories. They released a report on the ABPM trial [2] involving an African American female patient with severe hypertension but not currently taking any active medication. This test was conducted to determine the appropriate treatment and was performed by the Oscar 2™ automatic blood pressure monitor.

The report included 60 automated measurements and was created using AccuWin Pro 4. This user-friendly Windows application allows for the configuration, analysis, interpretation, and reporting of ABPM studies. The test started at 16:13 and finished the next day at 16:30. The sleeping time was in the range (23.00 - 7.00). The trials were hourly during sleeping; the diurnal ones had 20-minute intervals.

Exponential Smoothing Models

Exponential Smoothing Modeling (ESM) emerged in the second half of the last century as a forecasting method for time series data [16, 17, 19]. It posits that recent observations have a greater influence on the future values of a series than older ones. This method applies to time series that exhibit trends, seasonality, or both, as well as to those that lack these characteristics.

One of the branches of ESM is called "state space models," which includes Error-Trend-Seasonality (ETS) modeling. Each ETS model consists of a measurement equation that describes the data and some state equations that describe unobserved components or states (such as errors, level, trend, and seasonality) that change over time [17].

There are about 30 distinct ETS models, the details of which are described in the recently published book [16], resources [17], and paper [19]. Thus, any time series may be approximated by one of those. Various information criteria can be used here to determine which of the ETS models is most appropriate for a time series [14]. These are often the Akaike's Information Criterion, or the Bayesian Information Criterion. The method is programmed and implemented in many software, particularly Excel (since 2016), Maple (since 2018), and Python (since 2020) [17]. It is included in the "Time Series Analysis" package within Maple.

There are three main types of exponential smoothing. A simple method assumes no essential trends or seasonality, an extension that accounts for trends, and the most advanced approach supports both trends and seasonality [16]. Short series like ABPM exclude seasonalities.

Singular Spectrum Analysis

In [15], Singular Spectrum Analysis is explained in detail, especially its theoretical and computational foundations. SSA is viewed as a digital filter bank for biomedical signals [20]. SSA implementation within Maple was developed in [20] for a series with a short length of N = 128 points. However, the authors aim to apply SSA to ABPM, a much smaller series with only N = 24 samples.

A window length of $2 \le L \le 0.5N$ has a crucial meaning in this method. The point is that L defines the accuracy of trend extraction, and it is desirable to choose maximal $L = 0.5N$ [20].

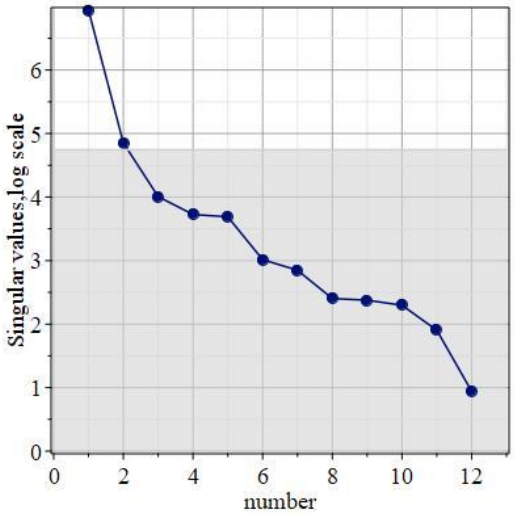


Fig. 1. Singular values of trajectory matrix for diastolic blood pressure series in the semi-logarithmic axes; those in a shadowed area are less than the mean value of the complete array

In Fig. 1, an array of singular values is displayed for the trajectory matrix corresponding to the series of diastolic blood pressure measurements from the ABPM. Similar diagrams are observed for the systolic and cardiac series. According to Kaiser's heuristic rule [15], ignoring all singular values and their right and left eigenvectors is recommended if the particular values are less than the mean of the array. For the diastolic and systolic blood pressure series, it is suggested that only the two highest singular values be considered. Aside from heart rate, even the highest singular value is enough.

Let $1 \le n \le L$ be the number of accounted singular values and $\{s\}_{i=1,\dots,L}$ the array of singular values. After that, the part of the total dispersion that ensures these selected values could be estimated as follows:

$$0 \le \alpha = \frac{\sum_{i=1}^{n} s_i^2}{\sum_{i=1}^{L} s_i^2} \le 1 \qquad (1)$$

The evaluations using expression (1) give 0.988, 0.998, and 0.993 for the heart rate, systolic, and diastolic pressure series of ABPM. One should remember that the quantities of accounted singular values (n) are equal to 1, 2, and 2, respectively. The highest singular values within SSA usually define the trends [9].

To characterize a complex system based on time series, trends, and fluctuations, these aspects should be studied separately. Detrended Fluctuation Analysis (DFA and similar methods [16, 17, 19]) enables the reliable detection of long-range (auto-) correlations and self-similarity in data, provided they exist. Their investigations help to find the series's persistence (or sometimes anti-persistence) and estimate their Hurst exponents [21].

Principal Component Analysis: short-time variabilities and recurrence plots

Blood Pressure (BP) is a highly dynamic parameter characterized by continuous fluctuations, including short- and long-term variability. Short-term variability within 24 hours can be readily assessed using ABPM [5], for instance, through the use of Poincaré Plots or Principal Component Analysis (PCA) [11, 12]. Different evidence from observational studies and post hoc analyses of data from clinical trials has indicated that cardiovascular events may also depend on increased short-term BP variability [5].

Estimating short-time BP variability can be a natural threshold for building informative recurrence plots for the ABPM series. These plots reflect the fundamental property of any life process, its relapsing (cycling) [22].

Trends

Trends enable us to estimate the average values required for clinical diagnostics more accurately (see Table 1). Note that the average values attained via different methods are almost identical. The heart rate unit is in bpm, while the BP unit is in mmHg.

Table1

Average values for ABPM series

Method	24-hours		Nocturnal	
	Heart rate	BP ratio	Heart rate	BP ratio
SSA	70	136/90	69	118/74
ETS	70	135/89	70	116/72

The night dipping of Table 1 is statistically significant at a confidence level of 0.99, as determined by a standard two-sample Z-test for 24-hour and nocturnal trials. The one exception is the heart rate trend, obtained via the ETS method, which shows no nighttime decrease in heart rate.

The similar results [2] concerning the night dipping are somewhat questionable. The dip in blood pressure observed in this report bordered on the respective standard deviations, which were overestimated in this method due to the impact of mixed fluctuations that were not separated from the sought signal. Meanwhile, our trends are free of such volatility.

Figure 2 illustrates the trends in heart rate and blood pressure ABPM series obtained using the SSA and ETS methods. They look similar but not identical. In particular, the SSA trends for blood pressure are much smoother than the analogous ETS trends. Besides, the SSA heart rate trend is not trivial compared to the ESM prediction

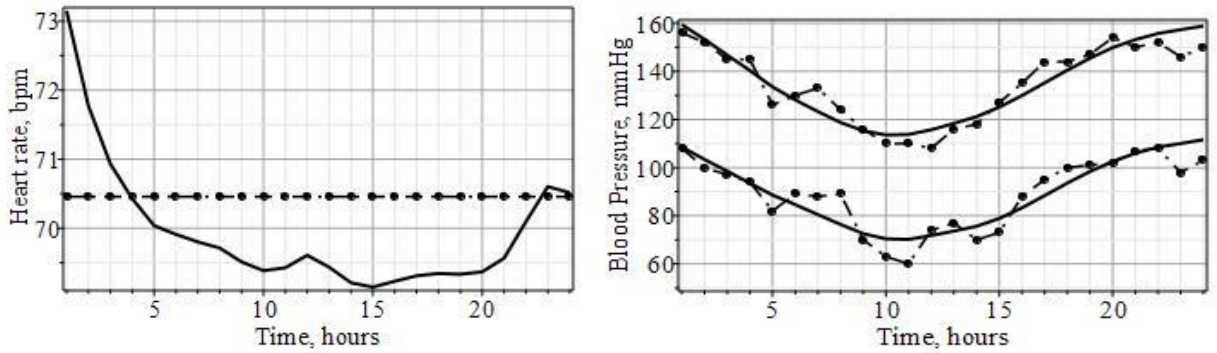


Fig. 2. Trends for heart rate (upper graph) and blood pressure (lower one); point lines show ETS trends, solid lines - SSA ones

Most trends in Fig. 2 have minima at nighttime. The one exception was mentioned above. Heart rate trends and BP ones have periodograms that show only one peak that matches the periodicity of about 24 hours. The SSA trends for blood pressure appear smoother than those of the ETS (Fig. 2).

Detrended fluctuations

The separation of detrended fluctuation allows for estimating their contribution to short-term heart rate and blood pressure variabilities. According to our SSA results, the heart rate, systolic blood pressure, and diastolic blood pressure show fluctuations of 6.5 bpm, 5.4 mmHg, and 6.0 mmHg, respectively. Similarly, ESM results indicate fluctuations of 6.7 bpm, 6.6 mmHg, and 7.7 mmHg, respectively. Comparing these results with the standard deviations reported in [2] of 7.0 bpm, 14.7 mmHg, and 13.2 mmHg, we can see that the fluctuation causes almost all of the heart rate variability and about half of the blood pressure uncertainty.

Detrended fluctuations reveal specific correlograms (autocorrelation functions); examples are shown in Figure 3. Results for BP are displayed there, but the correlogram for heart rate is similar to them.

All correlograms, regardless of whether obtained via SSA or ETS methods, exhibit decay with a power-law dependence on lags (L). It was confirmed in [22].

$$C(L) \sim L^{-\gamma}. \qquad (2)$$

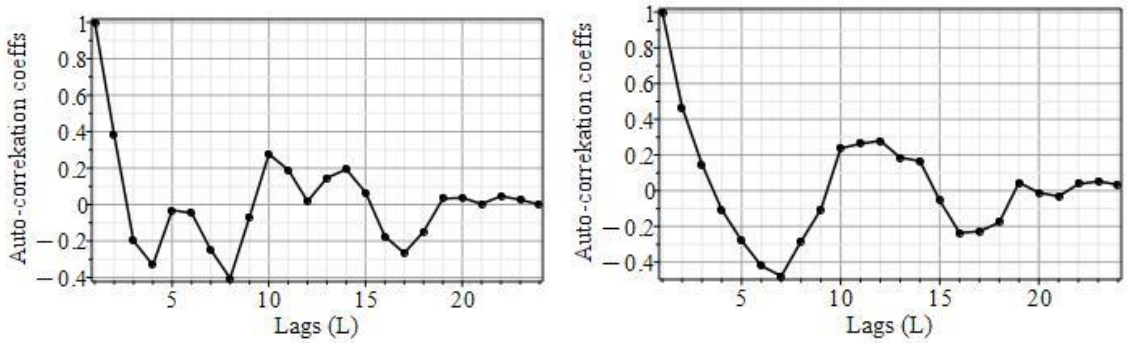


Fig. 3. Normalized correlograms for systolic (upper chart) and diastolic (lower diagram) arterial blood pressures; detrended fluctuations attained via the SSA method

Two other DFA exponents [22] are linearly connected with γ :

$$\alpha = 1 - \gamma / 2, \quad \beta = 1 - \gamma. \qquad (2)$$

The relations (3) are the straight consequences of the well-known Wiener-Khinchin theorem. At that, β defines the slope of power spectra ($P(f) \sim f^{-\beta}$), while α is an index of the noise "color."

The decay laws were found to be highly linear when examined on double-logarithmic axes. This excellent linearity is supported by the determination coefficients (R-squared values shown in Table 2). The DFA scaling exponents (α) are closely aligned across different series and methods of detrended fluctuation analysis. The inequality $\alpha \geq 0.5$ indicates that these series are fundamentally self-correlated, persistent, and exhibit "long memory."

Autocorrelation functions (correlograms) enable us to determine the power spectra of detrended fluctuations using the Wiener-Khinchin theorem, as demonstrated in the above-cited papers [20]. The power density is close but not identical for Detrended fluctuations attained via the SSA and ETS methods (see Figure 4). Spectra testifies that the series exhibits fluctuations with periods shorter than 24 hours, in contrast to the trends.

Table 2

DFA exponents and linearity estimators of the scaling power law in double-logarithmic axes

Meth.	SSA			ETS		
	HR	**SBP**	**DBP**	**HR**	**SBP**	**DBP**
α exp.	0.79	0.82	0.80	0.78	0.79	0.78
R^2	0.998	0.993	0.998	0.998	0.998	0.998

Note: HR, SBP, and DBP in Table 1 mean heart rate, systolic, and diastolic blood pressures, respectively.

Poincaré plots for the ABPM series have been examined in [11]. Our calculation, based on the method [12], confirms the earlier findings of [11]: short-term variabilities (SD1) are 6.5 bpm, 4.9 mmHg, and 5.7 mmHg, respectively. These thresholds enable the construction of matrices of similarity and recurrence plots. Fig. 5 displays examples of such plots for the detrended fluctuations of BP. One can see that SSA and ETS recurrence plots are alike but not identical.

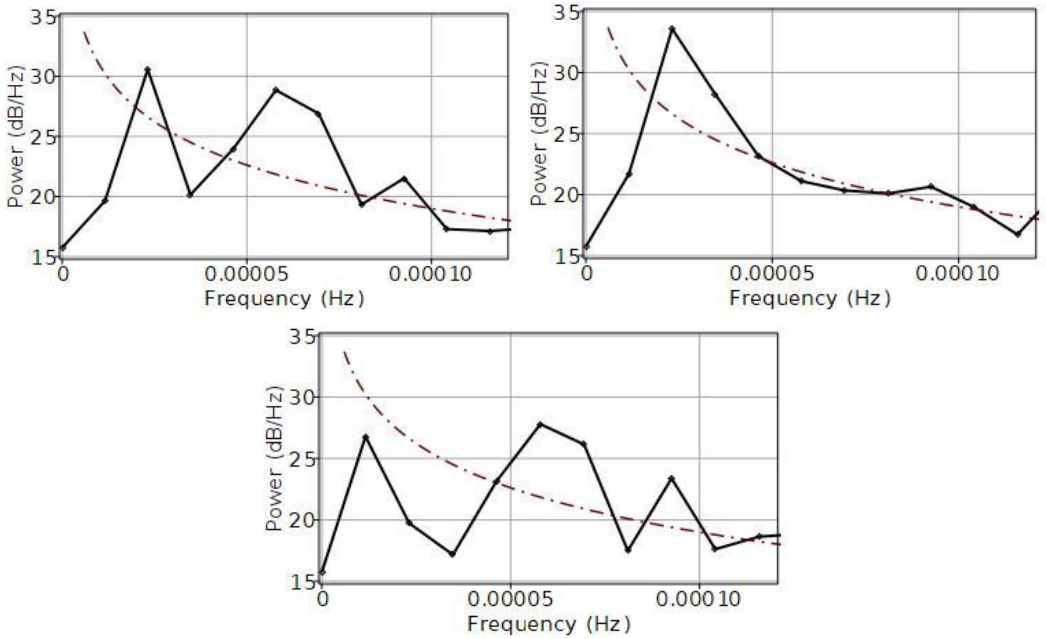


Fig. 4. Power spectra for blood pressures: systolic BP (left side) and diastolic one (right side); the upper row reflects the SSA method, while the lower one - ETS; solid lines are the power densities, dash-dot lines show the power-law decaying of power spectra with β=0.6, following (3) and data of Table 2

First, we can note that the results of two conceptually different methods (SSA and ETS) turned out so close. Similes within Section 3 demonstrated this convergence, which was not guaranteed a priori.

SSA does not predict specific time series structures ([15] and [20]) in contrast to ETS ([16, 17] and [19]. As a result, the partition of a time series strongly depends on the procedure of "singular triples grouping", which is partly an art based on experience and partly a technique.

The Kaiser's rule, used in this paper, is essentially a "rule of thumb." Another similar "thumb rule," the Cattell scree plot test [18], demands, for example, accounting for the first five singular values instead of two by Kiser's rule for Fig.1. We checked such a variant. As a result, some fluctuations are transferred to the trend, thus losing smoothness.

Perhaps the higher reliability of Kaiser's rule is due to the specific structure of the ABPM series. ETS claims that these series have the simplest possible model with additive noise, known as "simple exponential smoothing" [16]. There is no seasonality, but maybe a simple, smooth, undamped trend or no trend. Thus, the first few "singular triples" (one or two) might be enough to extract such a trend. Therefore, ETS modeling hints at "triples grouping" within SSA. They are excellent at working in "a couple."

The partition of the ABPM series into trends and fluctuations free of trend is possible via both methods, yielding close results. Note that SSA provides smoother trends, although it is slightly more labor-intensive. Purified trends, for instance, allow for a more reliable evaluation of 24-hour and nocturnal averages and night dipping because the noise-like components have been excluded from the valid signal.

Estimating the persistence of time series within ABPM is possible by analyzing detrended fluctuations. These time series have a long memory and are autocorrelated. However, it is not accurate to consider these fluctuations as Fractal Gaussian Noise (FGN) based solely on DFA exponent evaluations from Table 2. That is because FGN must have stationary increments and a power-law decay of its power spectra. In the best case, real power spectra (as shown in Fig. 4) are asymptotically close to the power-law decay.

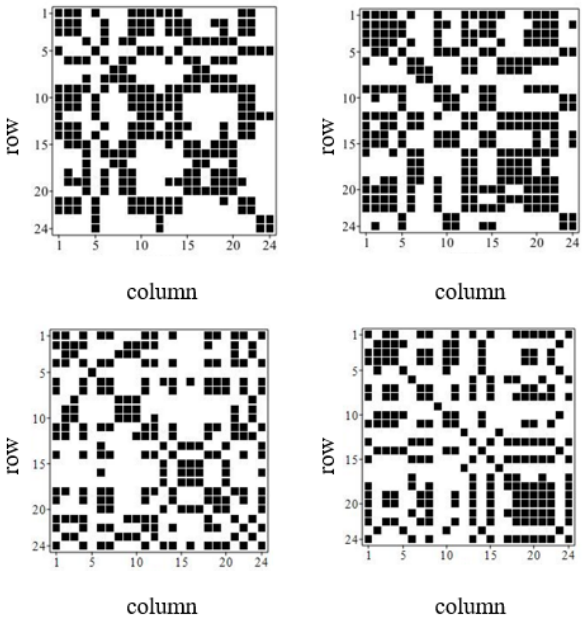


Fig. 5. Recurrence plots for detrended fluctuations: systolic BP (left-hand side) and diastolic one (right side); the upper row holds the SSA results, while the lower one – ETS: recurrence ratios are 0.451, 0.483, 0.389, and 0.402, respectively

Cleaned trend fluctuations also allow us to estimate short-range variabilities, which are the operative reactions of the blood circulatory system in an inconsistent habitat. Such variabilities can serve as the natural thresholds for the recurrence analysis of fluctuations.

The recurrence plots offer a range of exciting conclusions when one follows the qualitative analysis of [23]:

a) Many single isolated "pixels" testify to the dominance of heavy fluctuations or that ABPN is even partly stochastic and noisy.

b) Vertical and horizontal lines forming rectangles mean some states do not change or change slowly for some time (laminar states), or the process is halted at a singularity in which the dynamics are stuck in paused states.

c) Periodic patterns indicate that the process has characteristic cyclic ties, with periods corresponding to the time distance between periodic structures, which a circadian rhythm may cause.

d) SSA predicts a few higher recurrence rates than ESM concerning the ABPM systolic BP series.

Reliable SSA requires high-resolution data collected at least 30 minutes to one hour to monitor physiological responses effectively. The higher the temporal resolution of the time series, the more precisely we can distinguish the rapidly changing physiological components.

This limitation applies to ESM even more, as seen in Fig. 2, where this method demonstrates the lack of trend smoothness. Revising the standards for automated ABPM to shorten the intervals between consecutive tests may help overcome this limitation.

Discussion

As shown in Table 1, our results indicate a significant overestimation of the nocturnal pulse dip, with traditional processing reporting a seven-bpm increase compared to our measurement of no more than one bpm. Furthermore, the processing without partitioning [2] also notably exaggerates the 24-hour average blood pressure ratio (146/99 vs. our 136/89) and the nocturnal blood pressure dip (37-30 mmHg vs. 16-18 mmHg).

Detrended fluctuations provide additional valuable diagnostic information, including short-range BP variability [21] and persistence exponent. In particular, the Hurst Exponent evaluation testifies that it falls within the (0.5 – 1.0) range, with the most likely value being approximately 0.8. It indicates the persistent behavior of detrended fluctuations in the ABPM series, as well as some similarity with Fractional Gauss Noise, notably self-similarity and a power-law decay.

Additionally, fluctuations analysis offers insights into their power spectra and their similarity to fractional Gaussian noise (FGN). Understanding the nature of noise may improve the accuracy of ABPM trials in the future, for example, by employing noise filtering techniques. Knowledge of the short-time variabilities of BP became the basis for creating informative recurrence plots for the ABPM series.

Reliable SSA requires high-resolution data collected for at least 30 minutes to one hour to monitor physiological responses effectively. The higher the temporal resolution of the time series, the more precisely we can distinguish the rapidly changing physiological components.

This limitation applies to ESM even more, as seen in Fig. 2, where this method demonstrates the lack of trend smoothness. Revising the standards for automated ABPM to shorten the intervals between consecutive tests may help overcome this limitation.

Finally, the authors confidently assert that the primary objective of this research – reliably distinguishing between smooth trends and trend-free fluctuations in the ABPM series has been successfully achieved. The tasks specified in subsection 1.3 (a, b, c, and d) were executed with thoroughness and attention to detail, as supported by the preceding text.

Conclusions

Let us summarize the conclusions with a few points:

1. The ESM and SSA trends are truly close, but SSA ensures smoother curves
2. DFA analysis indicates the persistent behavior of detrended fluctuations in the ABPM, as well as similarity with Fractional Gauss Noise, notably self-similarity and a power-law decay/ ABPN are the series with "long memory"
3. The recurrence analysis reveals a relatively high recurrence rate for ABPM.
4. It would be helpful to decrease the intervals of measuring within standard ABPM to 30 minutes instead of one hour, and the number of trials increases to 48 per 24 hours.

References

1. Huang, Q.-F., Yang, W.-Y., Asayama, K., Zhang, Z.-Y., Thijs, L., Li, Y., O'Brien, E., & Staessen, J. A. Ambulatory Blood Pressure Monitoring to Diagnose and Manage Hypertension. *Hypertension*, 2021, vol. 77, iss. 2, pp. 254-264. https://doi.org/ 10.1161/hypertensionaha 120.14591

2. *Ambulatory Blood Pressure Report*. Available at: https://www.cardiacdirect.com/brochures/QRS_Opti_24_Hour_ABPM_Sample_Report_[Cardiac_Direct].pdf (accessed 29.06.2005).

3. O'Brien, E., White, W. B., Parati, G., & Dolan, E. Ambulatory blood pressure monitoring in the 21st century. *J Clin Hypertens*, 2018. vol.. 20, iss. 7, pp. 1108-1111. https://doi.org/ 10.1111%2Fjch.13275

4. Juraschek, S.P., Bello, N.A., Chang, A.R,. et al. Trends in Ambulatory Blood Pressure Monitoring in Five High-Volume Medical Centers. Hypertension. 2023; 80(8): e131-e133. https://doi.org/10.1161/HYPERTENSIONAHA.123.21412

5. O'Brien, E., Parati, G., & Stergiou, G. Ambulatory blood pressure measurement: what is the international consensus? *Hypertension*, 2013. vol. 62, iss. 6, pp. 988-994. https://doi.org/: 10.1161/hypertensionaha.113.02148

6. Carpena, P.; Gómez-Extremera, M.; Bernaola-Galván, P.A. On the Validity of Detrended Fluctuation Analysis at Short Scales. Entropy 2022, 24, 61. https://doi.org/10.3390/e24010061

7. Liu Ziyi; Zhou Congcong ; Wang Hongwei; He Yong. Blood pressure monitoring techniques in the natural state of multi-scenes: A review. *Frontiers in Medicine,* 2022, vol.9, https://doi.org/10.3389/fmed.2022.851172

8. Plug,J.G; Banegas J.R. ABPM in patients with heart failure: a long way to go. *Cardiologia,* vol.78,#11, pp. 841-842. https://www.revespcardiol.org/en-abpm-in-patients-with-heart-articulo-S1885585723002396

9. Castiglioni, P.; Omboni, S.; Parati, G.; Faini, A. Day and Night Changes of Cardiovascular Complexity: A Multifractal Multiscale Analysis. Entropy 2020, 22, 462. https://doi.org/10.3390/e22040462

10. Im, S.I.; Kim, Y.N.; Kim, H.S.; Kim, S.J.; Bae, S.H.; et all.. Hemodialysis Efficiency Predictor in End-Stage Kidney Disease Using Real-Time Heart Rate Variability. Biomedicines 2024, 12, 474. https://doi.org/10.20944/preprints202401.1181.v1

11. Chuiko, G., Dvornik, O., Yaremchuk, O., & Darnapuk, Ye. Ambulatory Blood Pressure Monitoring: Modeling and Data Mining. *Proceedings of the 1st International Workshop on Information-Communication Technologies & Embedded Systems (ICTES 2019),* Mykolaiv, Ukraine, November 14-15, 2019, vol. 2516, pp. 85-95. Available at: http://ceur-ws.org/Vol-2516/paper6.pdf (accessed 17.07.2023).

12. Chuiko, G., Dvornik, O., Darnapuk, Y., & Krainyk, Y. Principal Component Analysis, Quantifying, and Filtering of Poincaré Plots for time series typal for E-health. *Health Informatics: A Computational Perspective in Healthcare. Studies in Computational Intelligence*, 2021, vol. 932, pp. 61-76. https://doi.org/ 10.1007/978-981-15-9735-0_4

13. Khomidov, M.; Lee, D.; Lee, J.-H. A Novel Contactless Blood Pressure Measurement System and Algorithm Based on Vision Intelligence. *Electronics*, 2023, 12, 4898. https://doi.org/10.3390/electronics12244898

14. Gorban, A. N., & Zinovyev, A. Y. Chapter 2. Principal Graphs and Manifolds. *Handbook of Research on Machine Learning Applications and Trends: Algorithms, Methods, and Techniques*, Chicago, 2010, pp.28-59. https://doi.org/ 10.4018/978-1-60566-766-9

15. Poskitt D.S. On Singular Spectrum Analysis And Stepwise Time Series Reconstruction. *Journal of time series analysis Its Interface*, 2020, vol. 41, no. 1, pp. 67-94. https://doi.org/10.1111/jtsa.12479

16. Hyndman, R. J., & Athanasopoulos, G. Chapter 7. Exponential Smoothing. *Forecasting: Principles and Practice. 2nd edition*. OTexts Publ., 2018. 382 p. https://otexts.com/fpp2/ (accessed 17.07.2023).

17. Brownlee, J. *A Gentle Introduction to Exponential Smoothing for Time Series Forecasting in Python*. Available at: https://machinelearningmastery.com/exponential-smoothing-for-time-series-forecasting-in-python/ (accessed 12.04.2020).

18. Molkkari M; R¨as¨anen E. Robust Estimation of the Scaling Exponent in Detrended Fluctuation Analysis of Beat Rate Variability. *Computing in Cardiology*, 2018, vol 45, pp 1-4. https://www.cinc.org/archives/2018/pdf/CinC2018-219.pdf

19. Woo, G., Liu, C., Sahoo, D., Kumar, A., & Hoi, S. ETSformer: Exponential Smoothing Transformers for Time-series Forecasting. *arXiv:2202.01381*, 2022. 18 p. https://doi.org/ 10.48550/arXiv.2202.01381

20. Chuiko, G. P., Dvornik, O. V., Shyian, I. A., & Baganov, Ye. A. Trends and seasonality extracting from Home Blood Pressure Monitoring readings. *Informatics in Medicine Unlocked*, 2018, vol. 10, pp. 45-49. DOI: 10.1016/j.imu.2017.12.001

21. Hamza, A. H., & Hmood, M. Y. Comparison of Hurst exponent estimation methods. *Journal of Economics and Administrative Sciences*, 2021, vol. 27, iss. 128, pp. 167-183. https://doi.org/10.33095/jeas.v27i128.2162.

22. Chuiko, G., Darnapuk, Y., Dvornik, O., Yaremchuk, O., & Krainyk, Y. Recurrence Plots for Ambulatory Blood Pressure Monitoring: Means for Data mining of circadian rhythms. *IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT),* Zbarazh, Ukraine, 2020, pp. 80-83. https://doi.org/ 10.1109/CSIT49958.2020.9321837

23. Webber, Jr. C. L., & Marwan, C. *Recurrence Quantification Analysis – Theory and Best Practices*. Springer Cham Publ., 2015. 421 p. https://doi.org/10.1007/978-3-319-07155-8

Gennady Chuiko **Геннадій Чуйко**	D.Sc. in Physics and Mathematics, Professor of Computer Engineering Department, Petro Mohyla Black Sea National University Mykolayiv, Ukraine, e-mail: genchuiko@gmail.com https://orcid.org/0000-0001-5590-9404	д-р фіз.-мат. наук, професор кафедри комп'ютерної інженерії, Чорноморський національний університет ім. Петра Могили, Миколаїв, Україна.
Olga Yaremchuk **Ольга Яремчук**	PhD student, Department of Computer Engineering, Senior Lecturer of the Department of Medical Biology and Physics, Microbiology, Histology, Physiology, and Pathophysiology, Educational and Scientific Medical Institute, Petro Mohyla Black Sea National University Mykolayiv, Ukraine, e-mail: olga.yaremchuk.77@ukr.net https://orcid.org/0000-0002-0891-4216	аспірантка кафедри комп'ютерної інженерії, старший викладач кафедри медичної біології та фізики, мікробіології, гістології, фізіології та патофізіології Навчально-наукового медичного інституту, Чорноморський національний університет ім. Петра Могили, Миколаїв, Україна

https://doi.org/10.31891/csit-2025-2-9
UDC 004.052

PIKH Iryna, BILYK Oleksii
Lviv Polytechnic National University

WORKLOAD BALANCING IN THE TEST CASE SCHEDULING: A METHEMATICAL APPROACH

Efficient scheduling of test cases is a critical task in environments where execution resources, such as testers or test environments, are limited and subject to individual availability constraints. In this paper, we propose a flexible and extensible mathematical model for optimizing test scheduling based on discrete time blocks. Each test case has a fixed duration and must be assigned to exactly one compatible tester. Testers, in turn, may be unavailable at specific time blocks due to pre-scheduled meetings or fixed breaks, such as lunch. The scheduling objective is to minimize the makespan, defined as the latest finish time among all scheduled tests. The model is formulated as a mixed-integer linear programming (MILP) problem that integrates testers' compatibility and availability constraints with task assignments into a unified framework. In contrast to models that assume testers are always available or disregard personal schedules, our method incorporates individual availability constraints for more realistic planning. The model is assessed on a synthetic scenario involving multiple testers with defined break times and varying task compatibility, and the resulting schedule is visualized with Gantt charts. The proposed formulation serves as a foundation for more advanced scheduling systems in quality assurance and resource-constrained testing workflows.

Keywords: software testing, test case scheduling, resource allocation, mixed-integer linear programming, constrained optimization.

ПІХ Ірина, БІЛИК Олексій
Національний університет «Львівська політехніка»

БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ПРИ ПЛАНУВАННІ СЦЕНАРІЇВ ТЕСТУВАННЯ: МАТЕМАТИЧНИЙ ПІДХІД

Ефективне створення розкладу сценаріїв тестування є надзвичайно важливим завданням у середовищах, де ресурси для виконання, такі як тестувальники або тестові середовища, є обмеженими та доступними за індиввдуальними графіками. У цій статті запропоновано гнучку та масштабовану математичну модель для оптимізації розкладу тестування на основі дискретних часових блоків. Кожен тест-сценарій має фіксовану тривалість і повинен бути призначений одному сумісному тестувальнику. Тестувальники, у свою чергу, можуть бути недоступними у певні проміжки часу через заплановані зустрічі або фіксовані перерви, наприклад, обід. Метою планування є мінімізація загального часу виконання тестування, що визначається як найпізніший час завершення призначених тест-сценаріїв. Модель сформульовано як задачу змішаного цілочисельного лінійного програмування (MILP), яка об'єднує в єдиній структурі обмеження на сумісність та доступність тестувальників для призначення завдань. На відміну від моделей, які припускають постійну доступність тестувальників або не враховують їхні особисті розклади, наш метод враховує індивідуальні обмеження доступності для більш реалістичного планування. Для оцінки ефективності моделі використано синтетичні сценарії із декількома тестувальниками, визначеними періодами перерв і різною сумісністю завдань, а отриманий розклад подано через діаграми Ганта. Запропонована модель може слугувати основою для побудови більш складних систем планування у сфері тестування та контролю якості в умовах нестачі ресурсів.

Ключові слова: тестування програмного забезпечення, планування тестових сценаріїв, розподіл ресурсів, змішане цілочисельне лінійне програмування, оптимізація з обмеженнями.

Introduction

In modern software development lifecycles, testing plays a central role in ensuring product quality, system stability, and timely releases. As development processes accelerate under Agile and continuous integration frameworks, the pressure on test teams to deliver fast and thorough feedback increases. Testing must not only be accurate but also efficiently organized — particularly when multiple test cases must be assigned to limited testing resources under strict time constraints. Real-world testing environments introduce a number of challenges: testers and test environments are not always interchangeable, availability may be fragmented due to meetings or shifts, and time windows for testing are often constrained by sprint boundaries or release deadlines. As a result, manually constructing optimal test schedules that satisfy all technical and organizational requirements is both time-consuming and error-prone.

Previous research has explored test planning and resource allocation from various perspectives, including multi-sprint scheduling [1], metaheuristic test assignment [2], and architecture-driven reliability models [3]. Scheduling problems based on Mixed-Integer Linear Programming (MILP) have also been proposed for testing environments with complex resource constraints [4], [5], demonstrating their flexibility in encoding assignment, timing, and compatibility rules. Broader studies on test resource allocation [6], [7] emphasize the importance of optimizing test execution in terms of both efficiency and quality, while dynamic sprint replanning strategies [8] and modular software setups with change-point analysis [9] extend this line of research to more adaptive contexts. AI-driven solutions have also been investigated for resource-aware scheduling under uncertainty [10], incorporating intelligent heuristics and learning-based strategies. Several recent works address challenges closely related to our test scheduling model. Time-aware scheduling in shared-resource environments has been explored in cyber-physical

systems, highlighting the importance of precise execution under resource constraints [11]. Optimization-based sequencing using metaheuristics like particle swarm optimization targets similar goals of cost and time efficiency [12]. Dynamic test selection approaches, including just-in-time execution [13] and fuzzy prioritization [14], demonstrate the value of context-sensitive planning, though they often lack formal guarantees. Constraint-guided scheduling has shown strong industrial applicability in managing complex test environments [15], and large-scale case management efforts emphasize the need for robust tooling [16]. Complementing these efforts, systematic reviews provide a foundation for evaluating prioritization strategies [17]. Our work builds on these insights by offering a practical, extensible MILP-based model that unifies compatibility, availability, and non-overlap constraints to achieve balanced, time-efficient test schedules.

Despite these contributions, many existing models either assume continuous resource availability or do not explicitly incorporate structured calendars, shared breaks (such as lunch), or time-discretized execution windows. In practice, however, such factors are unavoidable. To address this, we propose a discrete-time MILP-based model that optimizes test case scheduling under personalized availability constraints. The model ensures that each test is assigned to a compatible tester in a way that respects all timing constraints while minimizing the overall makespan — the latest test finish time across all testers.

In this paper, we formally define the scheduling problem and present a MILP formulation that integrates resource-task compatibility, time discretization, and fixed unavailability periods. We validate our approach using a realistic synthetic scenario involving multiple testers, varied test durations, and non-overlapping availability schedules. The model is evaluated based on schedule compactness and total completion time, and results are visualized using block-based Gantt charts.

Problem Definition

We consider the problem of scheduling a set of software test cases over a working day, where each test must be assigned to a compatible tester within their available time. The objective is to minimize the makespan — the time at which the last test finishes — while ensuring no overlaps, respecting resource constraints, and accounting for structured unavailability such as meetings and lunch breaks.

Time is discretized into uniform blocks of size Δ (e.g., 15 minutes). The total number of blocks, denoted by T, depends on the duration of the working day. All tests are non-preemptive, meaning they must run to completion once started.

Let:

- I: Total number of test cases;
- K: Total number of testers;
- T: Total number of discrete time blocks in the scheduling horizon;
- d_i, $i = 1..I$: Duration of test case i, expressed in number of blocks;
- $c_{i,k} \in \{0,1\}$, $i = 1..I$, $k = 1..K$: Compatibility matrix — 1 if test case i can be executed by tester k, 0 otherwise;
- $A_{k,t} \in \{0,1\}$, $i = 1..I$, $t = 1..T$:Availability matrix — 1 if tester k is available at time block t, 0 otherwise (e.g., due to a fixed meeting or break);

We define binary decision variables $x_{i,k,t} \in \{0,1\}$, $i = 1..I$, $k = 1..K$, $t = 1..T$,: where $x_{i,k,t} = 1$ means that test case i is executed by tester k and starts at time block t. Additionally, we define $M \in R^+$ as the makespan, measured in minutes.

The model includes the following constraints:

- *Unique assignment*: Each test case must be scheduled exactly once
$$\sum_{k=1}^{K} \sum_{t=1}^{T} x_{i,k,t} = 1 \; \forall i = 1..I;$$
- *Compatibility*: Tests can only be assigned to compatible testers
$$x_{i,k,t} = 0 \; if \; c_{i,k} = 0 \; \forall i = 1..I, k = 1..K, t = 1..T;$$
- *Task duration feasibility*: No test may exceed the end of the working day
$$x_{i,k,t} = 0 \; \forall i = 1..I, k = 1..K, t \text{ such that } (t + d_i - 1) > T;$$
- *Tester availability*: No test case may be scheduled to start at a time that would cause it to exceed the scheduling horizon.
$$x_{i,k,t} = 0 \; if \; A_{k,\mathcal{T}} = 0, \mathcal{T} = t, .., t + d_i - 1, \forall i = 1..I, k = 1..K, t = 1..T;$$
- *No overlap*: A tester may run only one test at a time
$$\sum_{i=1}^{I} \sum_{t=1}^{T-d_i+1} \sum_{\mathcal{T}=t}^{t+d_i-1} x_{i,k,t} \leq 1 \; \forall k = 1..K;$$
- *Makespan definition*: the makespan must be greater than or equal to the end of any scheduled task
$$M \geq (t + d_i - 1) * \Delta * x_{i,k,t} \forall i = 1..I, k = 1..K, t = 1..T.$$

The objective is to minimize the overall makespan M, which corresponds to the completion time of the last scheduled test case. Thus, it is defined as

$$minM$$

By minimizing this value, the model encourages compact and efficient scheduling, improving test throughput and enabling faster integration or release cycles. This is especially valuable in time-sensitive development processes such as Agile sprints or continuous delivery pipelines.

Materials and Research Methods

This study applies a mathematical optimization framework to address the problem of scheduling test cases under resource constraints and individual availability limitations. The core methodology is based on a Mixed-Integer Linear Programming (MILP) formulation, which provides a rigorous and flexible means to encode scheduling decisions, compatibility constraints, and temporal limitations using a fully linear model.

To support the discrete execution of test cases, the working day is divided into a sequence of uniform time blocks of duration Δ (e.g., 15 minutes). All temporal aspects of the problem—such as test case duration, start and end times, and periods of unavailability due to meetings or breaks—are represented in terms of these blocks. This discretization allows the model to reflect real-world calendar constraints while maintaining computational efficiency.

The MILP model includes binary decision variables $x_{i,k,t}$, which indicate whether test case iii is assigned to tester k at time block t, and a continuous variable MMM representing the overall makespan, defined as the latest test completion time. The model enforces:

- unique assignment of each test case to one compatible tester;
- avoidance of overlaps in the schedule of any tester;
- exclusion of tasks from blocked periods (e.g., meetings, breaks);
- and minimization of the makespan.

All constraints and the objective function are expressed using linear relationships, enabling exact optimization with MILP solvers.

The model is implemented in Python using the PuLP optimization interface. We utilize the CBC solver (Coin-or branch and cut), an open-source MILP solver that integrates seamlessly with PuLP and supports both binary and continuous variables. Model construction and parameterization are fully automated. Feasible variable combinations are generated dynamically, based on test duration, tester compatibility, and availability. To interpret the resulting schedule, we generate visualizations using matplotlib and seaborn. The final output is rendered as a Gantt-style chart, with time plotted along the horizontal axis and testers along the vertical axis. Each test case is shown as a colored bar, labeled with its identifier, and fixed unavailability periods (e.g., lunch or meetings) are marked in gray. This provides an intuitive view of the scheduling outcome, workload distribution, and idle periods.

The proposed implementation supports configurable simulation parameters, enabling reproducibility and adaptation to various practical settings, such as full-day testing, sprint-bound scheduling, or load-balanced resource planning.

Experiments

To evaluate the effectiveness of the proposed scheduling model, we conducted two experiments with increasing complexity. In both cases, the goal was to assign test cases to testers in a way that respects fixed meeting times, avoids overlaps, and optimally utilizes the available workday. All tests were scheduled between 10:00 and 19:00 and split into 15-minute blocks. Each tester had a lunch break from 14:00 to 15:00, and additional fixed meetings that varied in number and timing.

Experiment 1: Two Testers with Long Tasks

In this scenario, 10 test cases of varying durations were distributed between two testers. Most tasks were compatible with both testers, although some were exclusive to one tester to introduce decision complexity. Each tester is also subject to availability constraints, including a mandatory lunch break and individual fixed meetings. The complete input data for this experiment is presented in Tables 1 and 2. Table 1 shows the test cases, their durations (in minutes), and the compatible testers. Table 2 presents the fixed meeting times for each tester, with all time values expressed in 24-hour format.

Table 1.

Description of the test cases for the first experiment: durations and compatibility with testers

Test Case	Duration (min)	Compatible Testers
Test A	135	Tester 1, Tester 2
Test B	60	Tester 1, Tester 2
Test C	90	Tester 1
Test D	120	Tester 1, Tester 2
Test E	90	Tester 2
Test F	75	Tester 1, Tester 2
Test G	75	Tester 1, Tester 2
Test H	75	Tester 2
Test I	60	Tester 1, Tester 2
Test J	45	Tester 1, Tester 2

Table 2.

Description of the testers fixed meetings for the first experiment

Tester	Event Start	Event End	Duration (min)
Tester 1	14:00	15:00	60
Tester 2	11:30	12:00	30
Tester 2	14:00	15:00	60
Tester 2	15:00	15:30	30

The resulting test schedule is illustrated in Figure 1. As shown, the optimizer respects all constraints and allocates tasks efficiently. Tester 1, with fewer interruptions, completes longer tasks and works until 19:00, while Tester 2, who has more frequent meetings, concludes by 18:15.

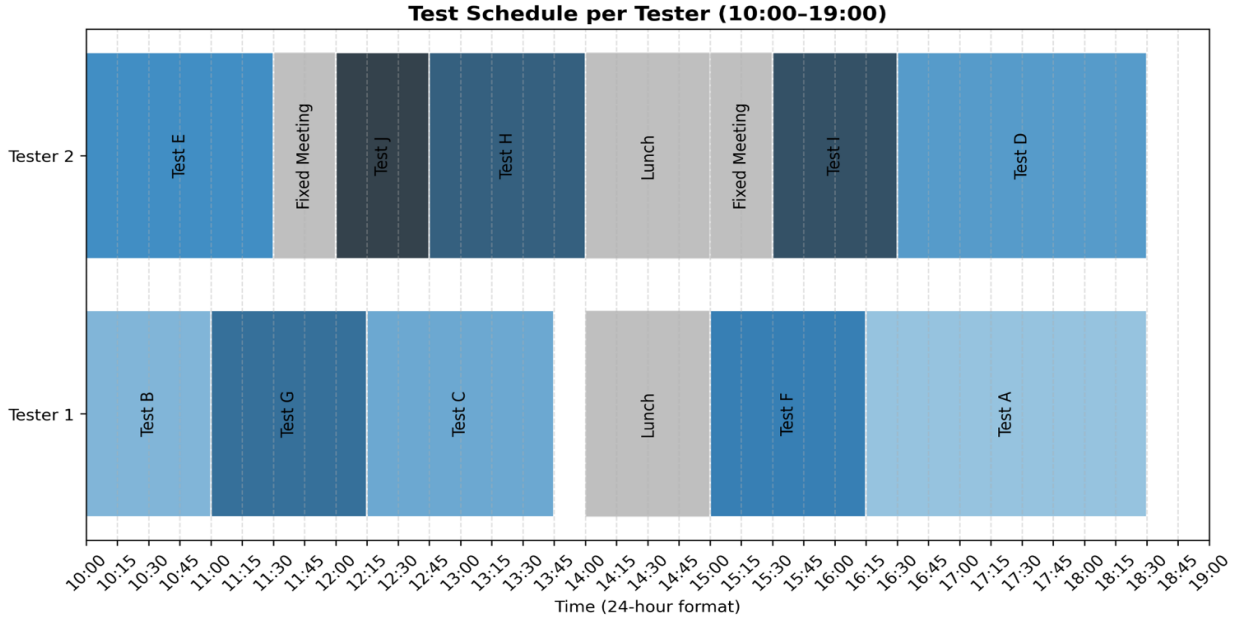


Figure 1. The first experiment. The optimized test schedule for two testers

Experiment 2: Three Testers with Denser Constraints

The second experiment increases the complexity to reflect more realistic, high-density team operations. It includes three testers and twenty-two test cases with diverse durations and a more intricate compatibility matrix. Many test cases are executable by multiple testers, though some remain exclusive. This setting mirrors real-world project scenarios where responsibility overlaps but expertise or permissions differ. Each tester has an individual schedule of fixed meetings throughout the day in addition to the shared lunch break from 14:00 to 15:00. The input configuration is summarized in Table 3 and Table 4.

Table 3.

Description of the test cases for the second experiment: durations and compatibility with testers

Test Case	Duration (min)	Compatible Testers
Test A	60	Tester 1, Tester 2
Test B	45	Tester 2, Tester 3
Test C	90	Tester 1
Test D	60	Tester 1, Tester 3
Test E	75	Tester 2
Test F	30	Tester 1, Tester 2, Tester 3
Test G	60	Tester 3
Test H	45	Tester 1, Tester 2
Test I	90	Tester 2, Tester 3
Test J	60	Tester 1, Tester 3
Test K	45	Tester 1
Test L	30	Tester 2, Tester 3
Test M	60	Tester 1, Tester 2, Tester 3
Test N	45	Tester 1
Test O	90	Tester 2
Test P	75	Tester 3
Test Q	30	Tester 1, Tester 2
Test R	60	Tester 2, Tester 3
Test S	45	Tester 2, Tester 3
Test T	30	Tester 1
Test U	60	Tester 2, Tester 3
Test V	45	Tester 1, Tester 2

Table 4.

Description of the testers fixed meetings for the second experiment

Tester	Event Start	Event End	Duration (min)
Tester 1	10:30	11:00	30
Tester 1	14:00	15:00	60
Tester 1	15:00	15:30	30
Tester 1	16:00	16:15	15
Tester 2	11:30	12:00	30
Tester 2	14:00	15:00	60
Tester 2	16:00	15:30	30
Tester 2	16:45	17:00	15
Tester 3	13:00	13:15	15
Tester 3	14:00	15:00	60
Tester 3	15:30	15:45	15

The optimized schedule is visualized in Figure 2, where the model demonstrates its ability to handle tightly packed constraints while maintaining balanced task allocation. All time constraints are satisfied, idle time is minimized, and resource usage is effectively distributed across testers without overlaps.

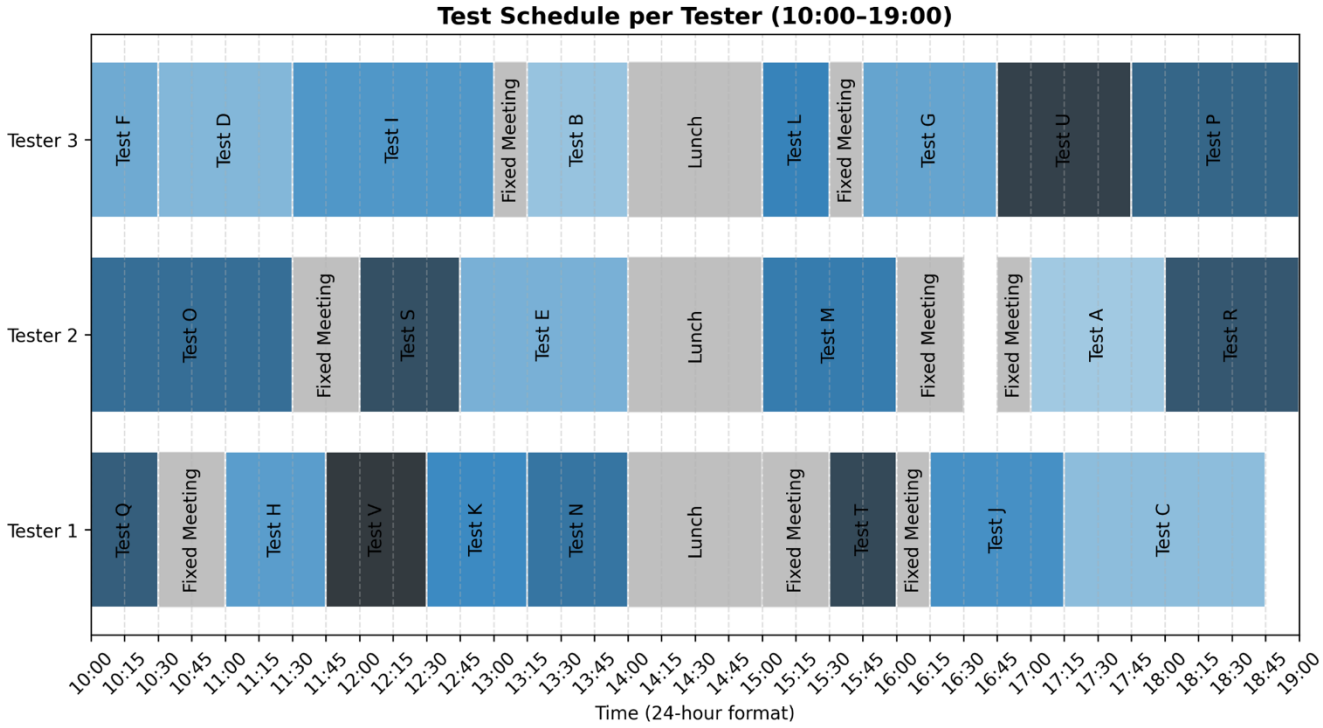


Figure 2. The second experiment. Optimized test schedule for three testers

Conclusions

This paper presented a mixed-integer linear programming approach for optimizing the scheduling of software test cases across multiple testers under realistic constraints. The model considers individual test durations, tester compatibility, and fixed availability windows, including meetings and lunch breaks. Time is discretized into fixed-length intervals, enabling precise formulation of scheduling rules and avoiding overlaps.

Two experiments were conducted to evaluate the model's effectiveness under different workload and availability scenarios. In both cases, the optimizer successfully generated feasible and compact schedules, respecting all compatibility and time constraints. The first experiment demonstrated the model's ability to efficiently allocate longer test cases to two testers with minimal idle time. The second experiment scaled up the problem to include three testers and twenty-two test cases, along with denser meeting schedules. The model remained robust and produced a tightly packed schedule with balanced task distribution.

The results confirm that formal optimization techniques can significantly improve the efficiency of test planning in constrained environments. By automating task allocation while incorporating practical constraints, the approach offers a valuable tool for test managers seeking to minimize idle time and makespan in real-world agile or sprint-based workflows.

Future work may explore the integration of test case priorities, dynamic availability, and non-linear objectives such as cost or risk balancing. The model can also be extended to support adaptive re-planning in the presence of runtime changes or execution delays.

References

1. Kumar, R., & Sharma, D. (2019). Software Testing Resource Allocation and Release Time Problem: A Review. International Journal of Software Engineering and Its Applications, 13(2), 47–64. https://www.researchgate.net/publication/333016163
2. Xie, Y., & Zhang, H. (2020). Search-Based Optimization for the Testing Resource Allocation Problem. Proceedings of the ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), 1–10. https://dl.acm.org/doi/10.1145/3383219.3383247
3. Pham, H., & Zhang, X. (2016). Optimizing Testing-Resource Allocation Using Architecture-Based Software Reliability Models. Software: Practice and Experience, 46(6), 751–768. https://doi.org/10.1002/spe.2356
4. Lopez, G., & Fernandez, J. (2018). Test Scheduling Using Mixed-Integer Linear Programming. International Journal of Advanced Computer Science and Applications, 9(11), 65–72. https://www.researchgate.net/publication/328614092
5. Cai, Y., & Yu, D. (2021). A Lagrangian Heuristic for Sprint Planning in Agile Software Development. Computers & Industrial Engineering, 157, 107291. https://doi.org/10.1016/j.cie.2021.107291
6. Garg, S., & Gupta, A. (2022). On the Testing Resource Allocation Problem: Research Trends and Perspectives. Journal of Systems and Software, 190, 111394. https://doi.org/10.1016/j.jss.2022.111394
7. Abelló, A., & Romero, O. (2020). Sprint Planning Optimization in Agile Data Warehouse Design. Journal of Intelligent Information Systems, 54(1), 65–84. https://doi.org/10.1007/s10844-019-00555-4
8. Pereira, C. R., & Figueiredo, A. A. (2022). Multi-Sprint Planning and Smooth Replanning: An Optimization Model. Journal of Systems and Software, 186, 111225. https://doi.org/10.1016/j.jss.2021.111225
9. Li, X., & Chen, J. (2020). A Study of Optimal Testing Resource Allocation Problem for Modular Software with Change Point. Journal of Software: Evolution and Process, 32(10), e2265. https://www.researchgate.net/publication/343675156
10. Zhou, Q., & Wei, Z. (2023). Software Testing Resource Scheduling Based on Artificial Intelligence. DiVA Portal – Uppsala University Publications. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1741041
11. Mossige, M., Gotlieb, A., Spieker, H., Meling, H., & Carlsson, M. (2019). Time-aware Test Case Execution Scheduling for Cyber-Physical Systems. *arXiv preprint arXiv:1902.04627*. https://arxiv.org/abs/1902.04627
12. Iqbal, Z., Zafar, K., Iqbal, A., & Khan, A. (2024). On Test Sequence Generation using Multi-Objective Particle Swarm Optimization. *arXiv preprint arXiv:2404.06568*. https://arxiv.org/abs/2404.06568
13. Amoroso d'Aragona, D., Pecorelli, F., Romano, S., Scanniello, G., Baldassarre, M. T., Janes, A., & Lenarduzzi, V. (2022). *CATTO: Just-in-time Test Case Selection and Execution*. arXiv preprint arXiv:2206.08718. https://arxiv.org/abs/2206.08718arXiv
14. Karatayev, A., Ogorodova, A., & Shamoi, P. (2024). *Fuzzy Inference System for Test Case Prioritization in Software Testing*. arXiv preprint arXiv:2404.16395. https://arxiv.org/abs/2404.16395arXiv
15. Gotlieb, A., Mossige, M., & Spieker, H. (2023). *Constraint-Guided Test Execution Scheduling: An Experience Report at ABB Robotics*. arXiv preprint arXiv:2306.01529. https://arxiv.org/abs/2306.01529arXiv
16. Kok, T. (2025). *Optimizing Test Case Management for Large-Scale Projects*. TestMonitor Blog. https://www.testmonitor.com/blog/optimizing-test-case-management-for-large-scale-projects
17. Singhal, S., Jatana, N., Suri, B., Misra, S., & Fernandez-Sanz, L. (2021). Systematic Literature Review on Test Case Selection and Prioritization: A Tertiary Study. *Applied Sciences*, 11(24), 12121. https://doi.org/10.3390/app112412121

Iryna Pikh **Ірина Піх**	Doctor of Technical Sciences, Professor, Professor of Virtual Reality Systems Department, Lviv Polytechnic National University, Lviv, Ukraine, e-mail: iryna.v.pikh@lpnu.ua https://orcid.org/0000-0002-9909-8444 Scopus Author ID: 57208669246 https://www.scopus.com/authid/detail.uri?authorId=57208669246	Доктор технічних наук, професор, професор кафедри систем віртуальної реальності, Національний університет «Львівська політехніка», Львів, Україна.
Oleksii Bilyk **Олексій Білик**	Post-Graduate Student, Lviv Polytechnic National University, Lviv, Ukraine; e-mail: oleksii.z.bilyk@lpnu.ua https://orcid.org/0009-0002-1355-2333	Аспірант, Національний університет «Львівська політехніка», Львів, Україна;

https://doi.org/10.31891/csit-2025-2-10
UDC 004.934:681.39

BOUHISSI Houda El, YURKO Pavlo
Khmelnytskyi National University

ANALYSIS OF BIOMETRIC ACCESS CONTROL SYSTEMS

The paper presents a method and a software-hardware tool for an access control system based on biometric data. The method involves the collection, processing, and verification of biometric features such as fingerprints, facial recognition, or iris scans to authenticate individuals. The system ensures secure access while minimizing the risks associated with traditional password-based security systems. The software-hardware tool integrates biometric sensors, data storage, and authentication algorithms to provide an efficient and secure means of controlling access to protected areas or resources. This approach aims to enhance security, streamline user access, and reduce the likelihood of unauthorized access or identity theft.

Keywords: biometric access control, biometric data, authentication, security system, software-hardware tool, fingerprint recognition, facial recognition, iris scan, identity protection.

БУХІССІ Худа Ель, ЮРКО Павло
Хмельницький національний університет

АНАЛІЗ СИСТЕМ КОНТРОЛЮ ПРОПУСКУ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

У статті представлено метод та програмно-технічний засіб для системи пропуску на основі біометричних даних. Метод включає збір, обробку та перевірку біометричних ознак, таких як відбитки пальців, розпізнавання обличчя чи сканування райдужної оболонки ока для аутентифікації осіб. Система забезпечує безпечний доступ, мінімізуючи ризики, пов'язані з традиційними системами безпеки на основі паролів. Програмно-технічний засіб інтегрує біометричні сенсори, зберігання даних і алгоритми аутентифікації, щоб забезпечити ефективний та безпечний контроль доступу до захищених територій або ресурсів. Цей підхід має на меті підвищення безпеки, спрощення доступу для користувачів і зменшення ймовірності несанкціонованого доступу чи крадіжки особистості.

Ключові слова: біометричний контроль доступу, біометричні дані, аутентифікація, система безпеки, програмно-технічний засіб, розпізнавання відбитків пальців, розпізнавання обличчя, сканування райдужної оболонки ока, захист ідентичності.

Introduction

Rapid advances in technologies such as digital cameras and portable video recording devices, as well as increased demand for security, make facial recognition technology a major biometric technology. There are many applications for facial recognition, including access control using mobile identity verification devices, mobile active video surveillance systems and rapid retrieval of records from remote facial databases[13]. With the standard authentication methods, such as passwords inheriting the vulnerabilities of being easily seen or stolen, the need for a new and better method was required. Biometric authentication was introduced as the method of protecting our info in our phones by using our biometrics, because it has a lesser chance of being stolen, as it’s impossible to completely steal all of the person's biometric data since there will always be something which won’t connect with the original.

Biometric authentication is one of the most secure forms of identification that can prove who we are. This cutting-edge technology uses our unique physical traits, such as fingerprints, facial features, or DNA, to verify our identity [1]. Due to the uniqueness of human biometrics witch played a master role in degrading imposters’ attacks. Such authentication models have overcome other traditional security methods like passwords and PIN [11]. With such authentication, protecting our identity in phones or in registrations is much easier than entering the password or making keys, since with huge amounts of registrations on different sites, and emails it is always required to have a password to protect the identity of the person. But with a huge amount of passwords, it is very hard to remember all of them, so it will take time and unnecessary work to make another one. There is always the chance that by saving all passwords in the memory bank of the device, it can be accidentally deleted or can be hacked and thus increasing the risk of security to be compromised.

Some of the potential risks associated with biometric authentication include: Appropriate technical and organizational measures, data breaches, false positives and negatives, forgery, user apprehension, regulatory compliance, longevity of biometric features.

To overcome these challenges, biometric authentication should be used carefully, implement strong security practices, and ensure compliance with relevant regulations. Additionally, using multi-factor authentication (MFA), which combines biometrics with other authentication factors, can provide an extra layer of security [2].

Domain analysis

In today's digital world, electronic devices, including biometric access systems, are becoming increasingly widespread. Examples of such technologies can be seen in embedded systems used in smartphones, Global

Positioning Systems (GPS) [3], and tablets. With the rapid development and extensive deployment of communication networks, millions of devices utilizing biometric data are connected to the global infrastructure.

Since users' personal data, including biometric information, may be accessible through the network, the need for protecting this data becomes critical. To ensure confidentiality and prevent unauthorized access, it is essential for access control systems based on biometric data to incorporate reliable software and hardware protection methods. This approach ensures a high level of security when using such systems in an open information environment.

Data protection methods, such as authentication and access control, are based on three key mechanisms:

(a) knowledge — information the user knows, such as passwords;

(b) tokens — physical items the user possesses, such as access cards or badges;

(c) biometrics — unique user characteristics, such as fingerprints, iris patterns, or movement dynamics [3].

The combination of these mechanisms forms multi-factor authentication, enhancing the reliability of security systems. For instance, biometric access control systems grant access to facilities or data using unique physiological traits of the user.

The integration of biometric technologies into access control systems significantly strengthens security by combining cryptographic techniques with biometric data analysis. Such solutions ensure accurate authentication, protection against unauthorized access, and the confidentiality and integrity of information, making them indispensable in modern software and hardware-based access control systems.

The process of verifying an individual's identity using unique physical or behavioral characteristics (such as facial features, fingerprints, hand structure, iris patterns, typing style, signature, or voice traits) is called biometric authentication [4]. This system provides a significantly higher level of protection compared to traditional password-based methods.

The main advantage lies in the necessity of the user's physical presence during authentication, which greatly complicates the possibility of unauthorized access. Additionally, there is no need to remember complex passwords or cryptographic keys, as biometric characteristics are naturally unique and inseparable from the individual. The verification mechanism works by comparing the current biometric data with the previously stored template created during registration [5].

The secure storage of these biometric templates is critical to the system's overall security, as biometric data cannot be changed or updated if compromised. However, research has shown that there are methods for stealing and replicating biometric data [6; 7], and the system may be vulnerable to malicious interference at various stages of the authentication process [8].

Biometric access systems are the systems that use unique physical characteristics data, such as fingerprints, facial recognition, or iris scans to identify individuals and grant them access to restricted areas of buildings [9]. They are used to determine the specific detail with each fingerprint or the detail on the face to recognize the particular person, as each of them have their individual details that make them unique and easily identifiable from the other people.

Biometric system has several components four components such as (Fig. 1) [9]:

- Input Interface (Scanners or Sensors);
- Processing Unit;
- Database Store;
- Output Interface.

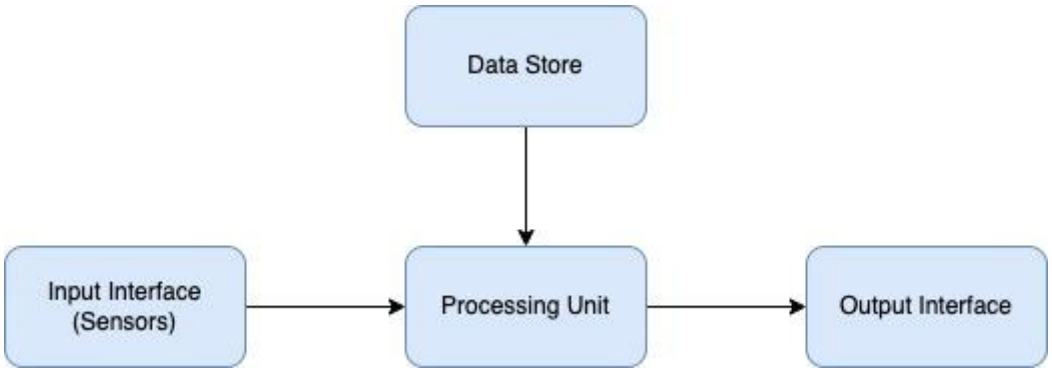


Fig.1. Biometric system components

No doubt biometric authentication increases security. However, biometrics are not immune to data breaches. If a malicious actor manages to get access to the database, then they get hold of the biometrics. This is not only a risk to the business, but it’s also a risk to the identity of workers as attackers can steal their biometrics for illegitimate purposes [10].

The risks of the usage of biometric data are to be expected, as there is nothing perfect and there is no 100% guarantee that the data and confidentiality are completely protected and no one can hack them. Most of the risks

include theft of biometric templates, misuse of the data by hackers or identity thieves, and even the possibility of falsification of the data also known as spoofing, which could be considered the most dangerous type of risk.

Fig 2. Distribution of Biometric System Components by Their Percentage Shares

Both security and privacy are important in the physical and digital worlds. Privacy is the right to control how the information is viewed and used, while security is protection against threats or danger. In the digital world, security generally refers to the unauthorized access of data, often involving protection against hackers or cyber criminals. Privacy consists of the person's right to manage their personal information, and security is the protection of this information. Both are equally important aspects of cyber safety. Everyone have the privacy rights and should take measures to secure their personal information and data within the digital environment [10].

Analysis of existing solutions and technologies

In today's fast-evolving digital landscape, biometric authentication systems have become increasingly prominent, providing robust security solutions. Several established technologies have been developed and deployed to enhance the security and efficiency of these systems. Here, we analyze the key existing solutions and technologies used in biometric authentication.

Fingerprint Recognition

Fingerprint recognition is one of the most widely used biometric modalities for authentication. It involves scanning the ridge patterns of a user's finger and comparing them against a stored template in the database. Many modern mobile devices and security systems use fingerprint scanners embedded in touchscreens or external sensors. Technologies like capacitive and optical scanners are commonly used in fingerprint recognition, offering quick and reliable identification. Despite its advantages, fingerprint recognition can be prone to spoofing through artificial fingerprints.

Facial Recognition

Facial recognition technology analyzes the unique features of a person's face, including the distance between eyes, nose shape, and overall facial structure. This form of biometric identification is increasingly employed in security systems such as smartphones, government identification programs, and surveillance cameras. 3D facial recognition and infrared sensors have advanced the robustness of this technology, improving accuracy even in low-light conditions. However, issues related to privacy, accuracy, and spoofing (e.g., using photos or videos to deceive the system) persist.

Iris Recognition

Iris recognition technology is based on the unique patterns in the colored part of the eye, providing a high level of security due to its uniqueness and stability. Unlike fingerprints or faces, the iris does not change over time, making it a reliable means of biometric identification. While iris recognition systems are accurate and fast, they are generally more expensive to implement and less commonly found in consumer devices compared to fingerprint or facial recognition systems. Despite the higher cost, iris recognition remains a favored choice for high-security applications, such as in government and military installations.

Biometric authentication technologies offer various advantages, depending on the use case. **Fingerprint recognition** is widely used due to its affordability and reliability, though it has vulnerabilities related to spoofing and fingerprint wear. **Facial recognition** is gaining popularity for its non-intrusiveness and versatility, but privacy

concerns and the potential for spoofing are significant drawbacks. **Iris recognition** offers high accuracy and robustness against spoofing but is less accessible due to high costs and less convenience.

Table 1

Comparison of Biometric Authentication Technologies

Biometric Technology	Description	Advantages	Challenges
Fingerprint Recognition	Scans the ridge patterns on a person's finger and compares them to stored templates. Used in mobile devices and security systems.	Widely available Fast and reliable Low-cost technology	Prone to spoofing (e.g., using artificial fingerprints) Can be less effective with damaged or worn fingerprints
Facial Recognition	Analyzes features of the face, such as distance between eyes, nose shape, and structure. Used in smartphones and surveillance systems.	Non-intrusive Fast and convenient Works in various environments (including low-light conditions with advanced tech like infrared)	Privacy concerns Spoofing with photos/videos Accuracy can be affected by facial changes or angles
Iris Recognition	Scans the unique patterns in the iris, providing high security due to the iris's stability over time. Typically used in high-security applications.	Extremely accurate Extremely accurate Stable over time Very difficult to spoof	High cost Less commonly used in consumer devices Can be less convenient (requires close proximity)

Definition of Similarity of Biometric Samples

Methods for comparing biometric templates typically involve calculating the similarity between two vectors that contain biometric data. Various mathematical models can be used for this.

Correlation:

One approach for comparing templates is calculating the correlation between two biometric data vectors is represented by the formula 1:

(1)

$$Correlation\ (X,Y) = \frac{\sum i = 1n(Xi - X^{-})(Yi - Y)}{\sqrt{\sum i = 1n(Xi - X^{-})2\sum i = 1n(Yi - Y^{-})2}}$$

Where Xi and Yi are the elements of the vectors X and Y (biometric samples), and bar X^{-} and Y^{-} are the mean values for each sample.

Euclidean Distance Method:

Another approach is using Euclidean distance, represented by the formula 2 which defines how similar two biometric templates are.

(2)

$$D,(X,Y) = \sqrt{\sum_{i=1}^{n}(Xi = Yi)2}$$

Where D(X, Y) is the distance between two biometric templates, indicating their similarity.

Biometric Authentication:

The authentication process involves checking the similarity between the current biometric data and the stored templates by the formula 3:

(3)

$$S = Similarity(X,Y)$$

Where S is the result of the comparison, indicating the level of similarity between the two biometric samples (from 0 to 1).

If S Threshold, authentication is successful, and access is granted to the user.

Calculation of the Probability of Successful Authentication and Error Rates are calculated by the formulas 4 and 5.

False Accept Rate (FAR):

(4)

$$FAR = \frac{Number\ of\ False\ Acceptances}{Total\ Number\ of\ Rejestions}$$

False Reject Rate (FRR):

$$FRR = \frac{Number\ of\ False\ Rejestions}{Total\ Number\ of\ Acceptancer} \quad (5)$$

Algorithms for Improving Accuracy

Filters are applied to biometric data samples to reduce noise, which enhances the accuracy of readings. This noise reduction is important for ensuring that the biometric system captures the most accurate and clean data possible. Various types of filters, such as median filters or Gaussian filter**s**, can be used to smooth out unwanted variations and artifacts, making the data more reliable for identification.

To ensure that biometric templates are stored accurately, methods like adaptive encoding and image processing are used. These techniques reduce data loss during the storage process, helping preserve the fidelity of the original biometric data. Adaptive encoding adjusts the way the data is encoded based on the characteristics of the sample, ensuring that relevant features are preserved while minimizing storage requirements. Image processing methods, such as contrast enhancement and edge detection, can also be applied to improve the quality of biometric samples before they are stored, ensuring higher accuracy in the later comparison stages. Biometric parameters differ in the cost, terms of efficiency and application. Differences in each parameter are presented in Table 2.

Table 2.

Analysis of Main Biometric SKUDs

Biometric Parameter	**Device Cost (USD)**	**False Acceptance Rate (FAR), %**	**Advantages**	**Disadvantages**	**Applicability for Detecting Authorized Operator Impersonation**
Fingerprint	100	0.001	High reliability. Resistance of the parameter. Small identification code. Compact reader. Low cost. Use of additional sensors (temperature, pressure).	Direct contact with the device. Complex algorithms. Easy to damage the fingerprint pattern. Quality depends on skin condition. Possibility of fingerprint forgery.	Used in mice, keyboards, laptops, mainly for authentication. Difficult to detect impersonation due to the need for continuous finger contact with the device.
Iris	>500	0.00001	Parameter resistance. High accuracy. Extremely difficult to fake. No direct contact with the device. High speed. Can be scanned from a distance.	Complex algorithms. High cost. Low availability of high-resolution solutions. Limited by eye alignment and scanning angle.	Difficult to apply for continuous monitoring, requires specific eye positioning towards the camera with small scanning angles.
Hand Geometry	>600	0.2	Parameter resistance. Simple algorithms.	Direct contact with the device. Inconvenient scanning procedure. Large size of the reader.	Continuous monitoring is impossible if the operator's hand is out of the scanner's range.
Retina	4000	0.000001	Unchanging over time. High accuracy. No direct contact with the device.	Difficulty in reading. Complex algorithms. High processing time for templates. High system cost.	Not applicable due to the need for specific conditions for reading the characteristic.
Face Geometry	>100	0.0047	Continuous authentication possibility. No direct contact with the device. Low cost.	Dependent on lighting conditions, head position. Sensitive to facial expressions. Sensitive to obstructions (glasses, hats, hairstyle changes).	Applicable for continuous monitoring, but with certain limitations due to the method's disadvantages.
Hand Veins	>300	0.0008	High accuracy. No direct contact with the device. Hidden characteristic.	Sensitivity to natural and artificial lighting. The characteristic depends on the state of the circulatory system.	Continuous monitoring is not possible if the operator's hand is out of the scanner's range.

Currently, there are many methods and approaches to facial recognition, each with its own characteristics and features. However, the fundamental principle of facial recognition remains common across all methods. The facial recognition algorithm involves creating a biometric model of the face for subsequent analysis and identification.

Typically, the structure of a facial recognition system consists of three main stages: the first is acquiring data about the face, the second is extracting distinguishing features, and the third is the actual recognition process. To do this, the object is fed into the system for identification, after which the face image is processed to extract key features, which are then used for verifying the identity [9].

Let's consider an example of such a process in a real-world case, where facial recognition methods are used in modern security systems.

However, upon further examination, the method of facial recognition consists of five key steps:

1. Face Detection.

The primary function of this step is to detect a face in the captured image. The face detection process essentially checks whether there is a face in the image. Once the face is identified, the result is passed on to the next step, which is preprocessing.

2. Preprocessing.

This step serves as the initial processing stage for facial recognition. During preprocessing, unwanted noise, blurring, varying lighting conditions, and shadow effects are removed using appropriate techniques. Once the image is smooth and clear, it is then ready for the feature extraction process.

3. Feature Extraction.

In this stage, facial features are extracted using a feature extraction algorithm. This process helps to condense information, reduce the image size, enhance brightness, and eliminate noise. After this step, the facial fragment is typically transformed into a fixed-dimensional vector or a set of points with their corresponding locations.

4. Face Recognition.

Once feature extraction is complete, the system analyzes the representation of the face. The extracted feature vector of the input face is compared with the stored faces in the database. If a match is found with sufficient confidence, the identity of the face is recognized; otherwise, the system indicates an unknown face [10].

The geometric method of facial recognition is one of the earliest approaches in this field. It involves detecting key points on the face, such as the corners of the mouth, eyes, and the tip of the nose, and using them to create a set of features. These features help identify a person by using geometric lines formed between the identified points (Fig. 2).

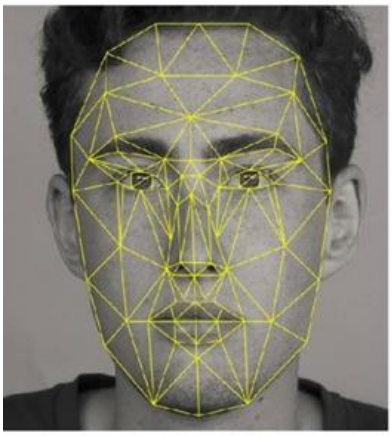


Fig. 2. Example of constructing geometric lines on a human face

The advantages of this method include the low cost of equipment and the ability to recognize faces from considerable distances. However, its drawbacks include high lighting requirements and the necessity for a frontal view of the person.

The method of elastic graph matching was also analyzed. It is based on comparing graphs that represent a facial image. These graphs consist of vertices and edges that describe the key facial features and their relationships. During recognition, one graph is fixed as the reference, while others deform to closely match the reference graph. This approach effectively handles variations such as changes in facial expressions, head movements, or distortions, making it a reliable method for face recognition (Fig.3).

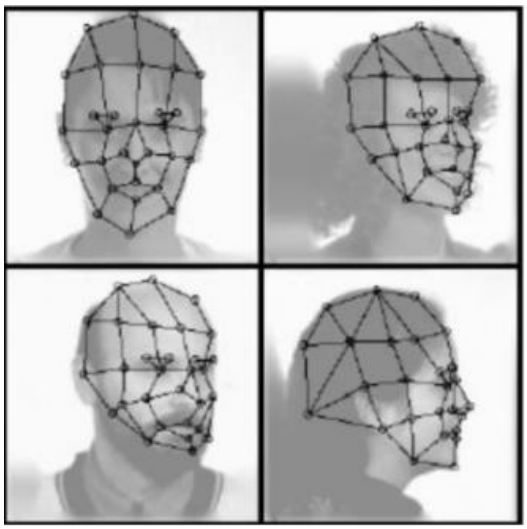


Fig. 3. Elastic Graph Matching Method

Each edge is defined by the distances between its vertices. For each point, the coefficients of the decomposition using Gabor functions with five different frequencies and eight orientations are calculated. This set of coefficients, J = {Jj}, is called a "jet." Jets describe local regions of the image and serve two main purposes: first, to find corresponding points in a given area on two different images; second, to compare the corresponding regions of different images. Each coefficient Jj = ajexp(iϕj) for points within the same region of different images is characterized by the amplitude aj, which changes gradually with the position of the point, and the phase ϕj, which varies at a rate proportional to the frequency of the wavevector of the basis function. In the simplest case, when searching for a point with similar characteristics in a new image, the phase is not considered in the similarity function.

The similarity function with a single jet at a fixed position and variable position is smooth enough to ensure fast and reliable convergence during the search using simple methods like gradient descent (GD). More advanced similarity functions incorporate phase information. For different angles, corresponding key points are manually marked in the training set. Additionally, to represent various variations of the same person's image in a single graph, multiple jets are used for each point, corresponding to different local characteristics of that point, such as open and closed eyes. The main advantage of this method is its low sensitivity to changes in lighting and facial angle [10].

There is also the Viola-Jones method, which is based on several key principles:

- ✓ It uses images in an integral form, allowing for quick computation of required objects.
- ✓ Haar features are used to search for the necessary objects.
- ✓ Boosting is applied to select the most suitable features in a given area of the image.
- ✓ The features are passed to a classifier, which outputs the result as either "True" or "False."
- ✓ Cascade features are used for quickly discarding windows where no face is found.

The algorithm works as follows: an image containing the desired objects is given. It is represented as a two-dimensional matrix of pixels with dimensions w*h, where each pixel has a value from 0 to 255 for grayscale images or from 0 to 255^3 for color images. The result of the algorithm is to detect the face and its features in the image, with the search carried out in the active region using rectangular Haar features. These features are used to describe the found faces and their characteristics: rectanglei={x, y, w, h, a}, where x, y are the coordinates of the center of the i-th rectangle, w is the width, h is the height, and a is the angle of the rectangle relative to the vertical axis of the image.

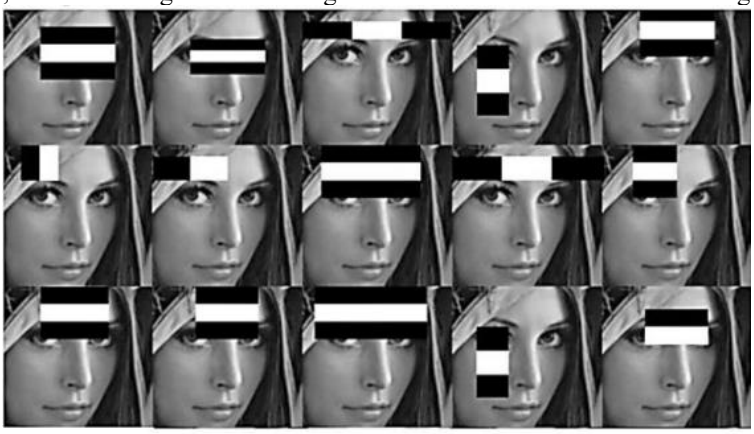


Fig. 4. Haar primitives

LeNet5 is a classic neural network architecture proposed by LeCun, originally designed for handwritten digit recognition. It consists of seven layers, with 60,000 learnable parameters and 345,308 connections. The reduction in the resolution of feature maps is achieved using subsampling layers. In a 2x2 subsampling filter network, the number of feature maps in a layer is halved, but it retains the same number of feature maps as the previous convolutional layer. LeNet5 accepts raw input images of size 32x32 pixels. It consists of three convolutional layers (C1, C3, C5), two subsampling layers (S2, S4), one fully connected layer (F6), and an output layer. The output layer is an RBF (Radial Basis Function) layer with 10 units for classification into 10 classes. The LeNet5 architecture can be applied to biometric data recognition in access control systems, where biometric features are used for user authentication.

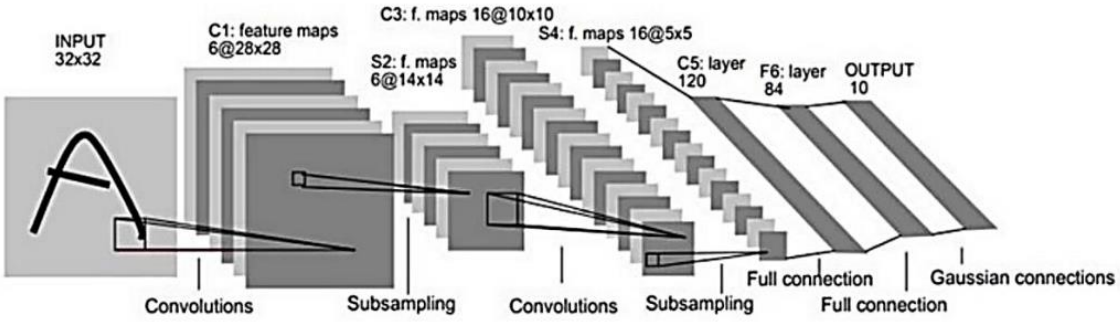


Fig. 5. Architecture of LeNet5

AlexNet is similar to LeNet but features deeper architecture with convolutional layers of sizes 11x11, 5x5, and 3x3. ReLU activation function is applied after each convolutional and fully connected layer (Fig. 6). The network aims to reduce training time and optimize performance for GPU usage, while also improving accuracy and overall efficiency. It achieves this by utilizing Rectified Linear Units (ReLU) and incorporating multiple GPUs. The introduction of these methods allowed AlexNet to significantly cut down training time and reduce errors, even with an increase in dataset size.

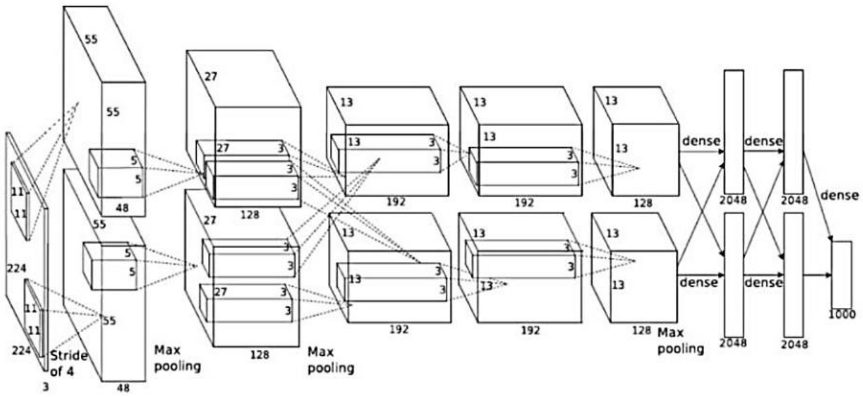


Fig. 6. Architecture of AlexNet

Residual Network (ResNet) is a type of CNN that can add extra layers to improve performance and accuracy. The added layers are capable of learning increasingly complex features, which correlates with better overall system performance and significantly improved image classification accuracy.

Practice shows that for average users who apply biometric identification and authentication systems, the convenience of using these tools is crucial. This involves not only the speed and simplicity of the procedure but also the ability to use existing equipment. Most experts agree that among various recognition methods, such as fingerprint, iris, or face recognition, three main methods are chosen based on the specific task. Today, facial recognition provides the optimal balance between authentication reliability, cost, and usability, which explains the rapid development and widespread adoption of such technologies.

A study of biometric access control and management systems was conducted. These systems are based on the recognition of physiological and behavioral characteristics of a person. The systems are classified depending on the type of characteristic they recognize.

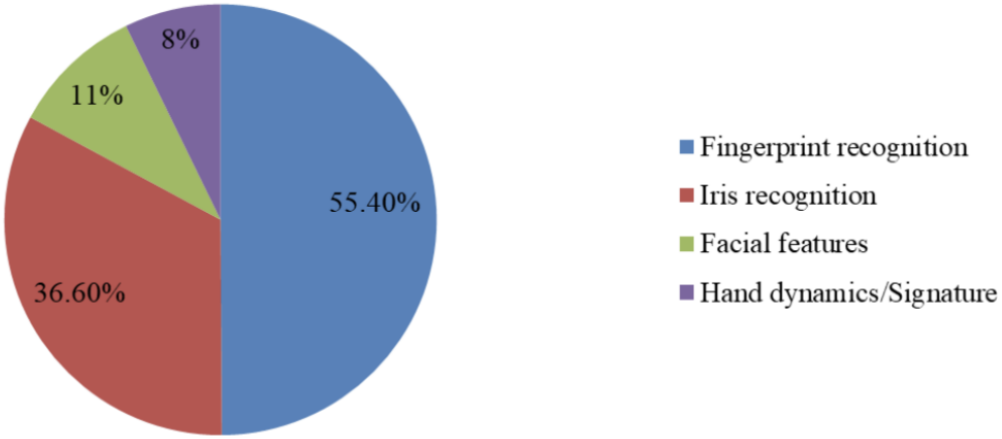


Fig.7. Distribution of Biometric Authentication Methods by Popularity

Based on the conducted analysis, it can be concluded that biometric systems using fingerprints, iris patterns, hand geometry, vein structure, and facial geometry have significant limitations in detecting the substitution of a legitimate user. These systems require specific conditions for scanning and may be ineffective for continuous monitoring. In particular, iris biometrics do not allow for continuous observation, as they also require specific conditions for scanning.

Therefore, for effective user substitution detection, it is most appropriate to use biometric characteristics that manifest during tasks the user typically performs. One of the most suitable options for continuous monitoring is keystroke dynamics, as this behavioral biometric most accurately reflects the individual traits of a user during computer interaction, particularly when typing or using a mouse.

Conclusion

In recent years, biometric technology has been vigorously promoted globally to enhance security in information technology (IT) and promote the development of emerging industries. Although biometric technologies have been employed in particular fields for a long time, they have gradually gained popularity to enhance the security of consumers and consumer electronics [12]. As a result of the analysis of modern biometric technologies and authentication methods, several important conclusions can be made. Biometric authentication is one of the most reliable and effective ways of identification, as it uses unique physical or behavioral characteristics of the user, making unauthorized access more difficult. Technologies such as fingerprint, facial, and iris recognition have their advantages and disadvantages, but combining these methods in multi-factor authentication provides an additional layer of security.

Despite their high reliability, biometric systems are not entirely immune to attacks and threats, such as theft of biometric templates or data forgery. Therefore, it is important to implement proper security measures and comply with privacy and security regulations. Given the convenience of using biometric technologies, especially facial recognition, their popularity and development are growing, opening new opportunities for improving the protection of personal data in various fields.

Overall, biometric authentication is a promising direction for ensuring security in the digital environment, but it is necessary to continually improve protection against potential threats and maintain a balance between security and user convenience.

References

1. Innovatrics, an EU-based provider based on biometric solutions. URL: https://www.innovatrics.com/glossary/biometric-authentication/ (Last accessed January 23, 2025)
2. Sumsub blog. URL: https://sumsub.com/blog/biometric-authentication-benefits-risks/ (Last accessed January 09, 2025)
3. Sangeetha, T., Kumaraguru, M., Akshay, S., & Kanishka, M. (2021, May). Biometric based fingerprint verification system for ATM machines. In Journal of Physics: Conference Series (Vol. 1916, No. 1, p. 012033). IOP Publishing.
4. Security Gallargather. URL: https://security.gallagher.com/en/Blog/An-Introduction-to-Biometric-Access-Control (Last accessed January 07, 2025)
5. Okta. URL: https://www.okta.com/identity-101/privacy-vs-security/ (Last accessed January 23, 2025)
6. Bio connect. URL: https://bioconnect.com/2024/08/01/6-ways-to-ensure-compliance-with-biometric-data-regulations/ (Last accessed January 07, 2025)
7. Terranova Security. URL: https://www.terranovasecurity.com/blog/hacking-biometrics (Last accessed January 09, 2025)
8. Analysis of Different Face Recognition Algorithms. URL: https://www.ijert.org/research/analysis-of-different-face-recognition-algorithms-IJERTV3IS111235.pdf (Last accessed January 09, 2025)
9. Face Recognition Using Neural Network: A Review. URL: https://www.researchgate.net/publication/301727666_Face_Recognition_Using_Neural_Network_A_Review (Last accessed January 09, 2025)
10. Face Recognition Methods: A Brief Overview. URL: http://itcm.comp-sc.if.ua/2017/Holubiak.pdf (Last accessed January 09, 2025)

11. A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. URL: https://www.sciencedirect.com/science/article/abs/pii/S2214785321048513 (Last accessed January 27, 2025).
12. Exploring biometric identification in FinTech applications based on the modified TAM. URL: https://link.springer.com/article/10.1186/s40854-021-00260-2 (Last accessed January 27, 2025).
13. An Ensemble Approach To Face Recognition In Access Control Systems. URL: https://journals.riverpublishers.com/index.php/JMM/article/view/24241 (Last accessed January 27, 2025).

Худа Ель Бухіссі **Houda El Bouhissi**	PhD, Associate Professor, LIMED Laboratory, Faculty of Exact Sciences, University of Bejaia, 06000 Bejaia, Algeria, e-mail: houda.elbouhissi@gmail.com https://orcid.org/0000-0003-3239-8255	доктор філософії, доцент, лабораторія Лімед, факультет точних наук, університет Беджайя, 06000 Беджайя, Алжир.
Pavlo Yurko **Павло Юрко**	Student of Computer Engineering & Information Systems Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: pavel.yurko.7654@gmail.com	студент кафедри комп'ютерної інженерії та інформаційних систем, Хмельницький національний університет, Хмельницький, Україна.

https://doi.org/10.31891/csit-2025-2-11
UDC 004.8

MOLCHANOVA Maryna
Khmelnytskyi National University
DUTT Pawan Kumar
Tallinn Technical University (Estonia)

ARTIFICIAL INTELLIGENCE APPROACH TO IDENTIFYING PROPAGANDA TECHNIQUES AND OBJECTS, TAKING INTO ACCOUNT ETHICAL AND LEGAL ASPECTS

The article explores the ethical and legal aspects of applying artificial intelligence (AI) technologies to detect propaganda techniques in textual content. The study presents a multi-level approach to identifying signs of propaganda in textual data, recognizing common rhetorical strategies of influence, and establishing semantic links between the detected techniques and their respective targets. The consistent use of neural network models is justified, as it ensures both classification accuracy and transparency of the obtained results through the application of local interpretability methods. The paper presents experimental results based on a corpus of Ukrainian-language news texts and informational messages from social media platforms. The proposed approach demonstrated alignment between the model's predictions and independent expert assessments, confirming its potential applicability in conditions with limited human oversight.

Special attention is given to the compliance of the proposed system with existing regulatory frameworks, including constraints on automated decision-making, the user's right to explanation, and the prevention of discriminatory effects resulting from biased training data. The study addresses risks associated with misclassification, potential impacts on freedom of expression, and the accountability of developers in cases where the system is applied in automated content moderation scenarios.

The integration of interpretability tools into neural network analysis is proposed as a core design principle to ensure adherence to ethical AI standards. Based on the obtained findings, the study concludes that the development of such systems requires the simultaneous consideration of technical effectiveness, legal compliance, and social responsibility, which are essential conditions for their safe implementation in the practice of analyzing public communications.

Keywords: artificial intelligence, ethical aspects, legal regulation, propaganda detection, natural language processing, neural network models, model interpretability, automated decision-making, information security, content moderation.

МОЛЧАНОВА Марина
Хмельницький національний університет
ДАТТ Паван Кумар
Талліннський технічний університет (Естонія)

ПІДХІД ВИКОРИСТАННЯ ЗАСОБІВ ШТУЧНОГО ІНТЕЛЕКТУ ДО ІДЕНТИФІКАЦІЇ ПРИЙОМІВ ТА ОБ'ЄКТІВ ПРОПАГАНДИ З ВРАХУВАННЯМ ЕТИЧНИХ ТА ПРАВОВИХ АСПЕКТІВ

Стаття присвячена дослідженню етичних та правових аспектів застосування технологій штучного інтелекту (ШІ) для виявлення пропагандистських прийомів у текстовому контенті. У роботі розглядається багаторівневий підхід до виявлення у текстових даних ознак пропаганди, визначення типових риторичних технік впливу та встановлення зв'язків між ідентифікованими прийомами й об'єктами впливу.

Обґрунтовано послідовне застосування нейромережевих моделей, яке забезпечує як точність класифікації, так і прозорість отриманих результатів за рахунок використання локальної інтерпретації результатів. Наведені результати експериментального дослідження на корпусі україномовних новинних повідомлень та інформаційних повідомлень з соціальних платформ. Запропонований підхід продемонстрував відповідність результатів передбачення оцінкам незалежних експертів, що підтверджує можливість його застосування в умовах обмеженого людського контролю.

Особливу увагу приділено відповідність функціонування запропонованого підходу чинному нормативному регулюванню, включаючи вимоги щодо обмеження автоматизованого прийняття рішень, права користувача на пояснення, а також запобігання дискримінаційним ефектам на основі упереджених даних навчання. Розглянуто ризики, пов'язані з хибною класифікацією, потенційним впливом на свободу вираження поглядів, а також відповідальністю розробника у разі використання системи в автоматизованих рішеннях, що стосуються контентної модерації.

Запропоновано інтеграції засобів пояснюваності як складової при нейромережевому аналізі, що дозволяє забезпечити дотримання принципів етичного ШІ. На основі отриманих результатів зроблено висновок, що розробка таких систем потребує одночасного врахування технічної ефективності, нормативно-правового супроводу та соціальної відповідальності, що є необхідною умовою їх безпечного впровадження у практику аналізу публічних комунікацій.

Ключові слова: штучний інтелект, етичні аспекти, правове регулювання, виявлення пропаганди, обробка природної мови, нейромережеві моделі, пояснюваність моделей, автоматизоване прийняття рішень, інформаційна безпека, контентна модерація.

Introduction

In today's digital environment, the spread of propaganda via text messages on social networks and news platforms poses a serious threat to information security and societal stability. Thanks to their ability to process large amounts of data and detect hidden patterns, artificial intelligence systems have become an effective tool for automatically detecting propaganda techniques in natural language texts. However, the implementation of such

systems raises a number of ethical and legal issues related to the transparency of algorithms, model bias, respect for human rights and regulatory requirements.

As stated in the requirements of the General Data Protection Regulation (GDPR) [1], an individual is guaranteed the right not to be subject to a decision based solely on automated processing if it significantly affects his or her rights and freedoms (Article 22). The EU AI Act [2] states that systems used to assess or influence public sentiment may be classified as high-risk systems. Such systems must meet the requirements of transparency, explainability, non-discrimination, and provide for the possibility of auditing and appealing automated decisions.

Also, ethical frameworks are defined in documents such as: OECD AI Principles [3], UNESCO Recommendation on the Ethics of Artificial Intelligence [4], Human Centric AI: A Comment on the IEEE's Ethically Aligned Design [5].

In the legislation of Ukraine, there is a lack of a clearly formulated regulatory framework for the use of AI in the field of information security, which creates challenges in adapting European standards to Ukrainian realities. However, at the level of state initiatives, in particular within the framework of the Government Action Plan for 2024 [6], the need to strengthen the capacity to counter information threats has been emphasized.

Thus, modern technical solutions in the detection of propaganda, although they demonstrate high potential, require support by regulatory and ethical mechanisms that ensure a balance between accuracy, transparency and user rights.

The main contribution of the paper is the proposed approach to ensuring transparency and explainability of deep learning model decisions, methods for minimizing algorithmic bias, as well as compliance with legal norms regarding the processing of personal data and automated decision-making. Particular attention is paid to the development of system architecture that combines the effectiveness of propaganda detection with compliance of ethical principles and legal requirements.

Further, the structure of the paper is as follows: the section «Literature review» provides an overview of the current state of the scientific direction of responsible and explained artificial intelligence in terms of solving the problem of detecting propaganda influences; the section «Proposed approach» provides an approach to implementing multi-level processing of text content to detect propaganda techniques and corresponding objects of influence; the section «Results and discussion» presents the results of an experimental study of the effectiveness of the developed approach on Ukrainian-language text corpora, including metrics of classification accuracy, interpretation quality and compliance of conclusions with experts' expectations, and also discusses the feasibility of practical application of the system in conditions of increased ethical requirements; The final section «Conclusions» summarizes the main scientific provisions of the study, outlines the potential of the proposed approach for further research in the field of responsible artificial intelligence and its use in the field of information security.

Literature review

Much of the current research on propaganda detection in natural language texts is based on the application of deep learning methods and transformative architecture models, such as BERT, RoBERTa, and DeBERTa. In particular, within the framework of the SemEval-2020 Task 11, it was proposed to classify 14 propaganda techniques in news content, which became the basis for many subsequent approaches to the automated detection of manipulative techniques. In [7] and [8], it is noted that deep models demonstrate high accuracy, but are limited in the explainability of their decisions. The authors of [9] investigate the vulnerability of pre-trained language models, such as BERT, to attacks using deliberate text modification aimed at manipulating the results of propaganda detection. The main attention is paid to the use of explainable artificial intelligence (xAI) tools, in particular SHAP and LIME, to identify keywords in texts that most affect the model's decisions. A similar study was also conducted by the authors [10], however, coalitional game theory approaches were used here, which allowed us to analyze the contribution of each linguistic characteristic to the final evaluation of the text, as well as to derive a general linguistic profile of propaganda in the American media. Unlike the previous study, which investigated how vulnerable the models are to changes in critical words identified by xAI methods in order to assess their resistance to deliberate attacks, here the focus is on explaining the model's decisions through the interpretation of linguistic features that shape the propaganda message.

The authors of [11] emphasize that although modern artificial intelligence algorithms, in particular deep and machine learning methods, demonstrate high performance in many applied tasks, their opacity and tendency to biased decisions create serious ethical and practical challenges. These algorithms often operate as "black boxes", which makes it difficult to interpret the results, especially in the context of complex and sensitive tasks related to social discourse analysis. In this context, the potential of XAI is explored, which provides new tools for interpreting and explaining the decisions of machine learning models. The authors analyze XAI as a promising approach to increase the transparency of systems that detect destructive online content, in particular hate speech and disinformation.

In our own previous studies [12], we point out the importance of marker-oriented approaches, where the use of semantic features allows us to link certain linguistic structures with specific propaganda techniques. In such approaches, visual analytics plays an active role, which improves the interpretability of the results [13].

Despite the rapid development of artificial intelligence tools, the use of deep language models to detect propaganda is accompanied by a number of significant limitations. These include insufficient transparency of decisions, the risk of algorithmic bias, and the inconsistency of individual technical solutions with modern ethical and legal requirements. Existing approaches focus mainly on increasing the accuracy of classification or on studying the vulnerabilities of models to manipulative attacks, but they do not pay attention to the issue of ensuring the interpretability of the results in the context of compliance with the principles of digital justice, user rights protection, and regulatory soundness.

Therefore, based on the above analysis of existing solutions, the purpose of research is to substantiate the conceptual foundations and principles of implementing the multi-level approach to identifying propaganda techniques and objects of influence in text content, taking into account the requirements for transparency, explainability and responsibility of decision-making.

To achieve the set goal, the following research tasks must be performed:

1. To substantiate the architectural and conceptual principles of a multi-level approach to identifying propaganda techniques and objects of influence in text content, taking into account the principles of transparency, explainability and ethical responsibility.
2. To implement a model of primary classification of texts by the presence of signs of propaganda, using neural network technologies and a probability scale for differentiating messages by the degree of severity of manipulative influence.
3. To develop a methodology for identifying propaganda techniques at the level of semantic interpretation, using marker-oriented analysis and built-in means of visual interpretation of results.
4. To propose the approach to identifying objects of propaganda influence, which involves semantic grouping and establishing logical connections between rhetorical techniques and target concepts mentioned in the text.
5. To ensure transparency and explainability of model solutions by integrating local interpretation tools, as well as verify their effectiveness by comparing them with expert assessments.
6. To assess the effectiveness of the proposed system in real-world applications, in particular in the field of information security, to increase user trust and compliance with legal and ethical standards.

Proposed approach

The research proposes approach that implements multi-level processing of text content to identify propaganda techniques and corresponding objects of influence. The approach (Fig. 1) consists in decomposing the initial task of detecting a text containing propaganda, taking into account the requirements for transparency, explainability and responsibility of the decisions made, into successive tasks:

(1) initial classification of the text for the presence or absence of signs of propaganda;

(2) semantic interpretation of the techniques, with the identification of specific rhetorical or psychological techniques inherent in the propaganda discourse;

(3) detection of objects of influence aimed at identifying the goals of propaganda influence and establishing their connection with the corresponding techniques.

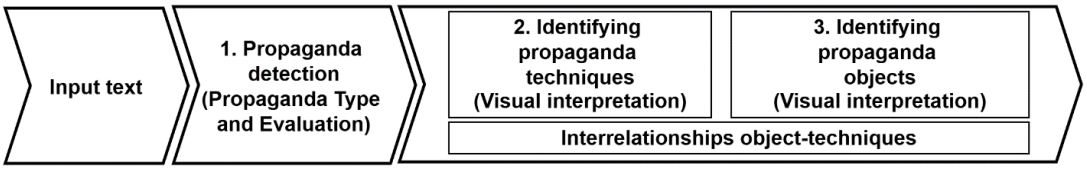


Fig. 1. General scheme of the approach to identifying propaganda techniques and objects

The input data of proposed approach is a text message.

Next, using pre-trained deep learning models, for the first task, using a binary classifier with a probable result, it is determined whether the text contains signs of propaganda, classifying messages by the level of probability into one of the categories: “non-propaganda”, “suspicious” or “propaganda”. If the probability of influence is detected, then we proceed to the second task.

The second task is responsible for detecting propaganda techniques and their visual interpretation. It is used only for texts classified as «propaganda text». The input text is fed in turn to 17 trained neural network models to analyze the presence of 17 propaganda techniques [14, 15, 16]:

1. «Appeal to fear-prejudice».
2. «Causal Oversimplification».
3. «Doubt».
4. «Exaggeration».
5. «Flag-Waving».
6. «Labeling».
7. «Loaded Language».

8. «Minimisation».
9. «Name Calling».
10. «Repetition».
11. «Appeal to Authority».
12. «Black and White Fallacy».
13. «Reductio ad hitlerum».
14. «Red Herring».
15. «Slogans».
16. «Thought terminating Cliches».
17. «Whataboutism».

Accordingly, the output data will be an assessment of the presence of propaganda techniques by markers [17] and a visual interpretation of the results [18].

The third task is responsible for detecting propaganda objects and their visual interpretation. It uses the results obtained during the implementation of previous methods. It transforms the input data into a set of thematic propaganda objects with the relationships of the detected objects with propaganda techniques.

Thus, the proposed approach not only ensures the detection of propaganda, but also meets the requirements for ethical responsibility: in particular, the transparency of models, the user's right to explain the results and the verifiability of the connections between influence techniques and the objects of their application.

Results and discussion

For the proposed approach, an experimental research was conducted to assess the effectiveness of propaganda detection, classification of its techniques, and identification of influence objects, with an emphasis on transparency and interpretation of the obtained solutions.

Text classification by propaganda content, using a hybrid model based on BiLSTM [19] with an additional level of attention, showed on test datasets an F1-measure value of 0.91 when classifying Ukrainian-language texts included in the corpus of news and social messages. The value of the Recall metric (0.93) confirmed the model's ability to identify even weakly expressed forms of manipulative influence.

Recognition of propaganda techniques, using a model based on markers and the BERT architecture [20], showed effective differentiation between 17 classes of rhetorical techniques. F1-measure values in the range of 0.82–0.88 were obtained for the main categories («Appeal to Fear», «Loaded Language», "»Name Calling»), which confirms the ability of the system to detect stable patterns even in stylistically heterogeneous texts.

When identifying objects of influence, the results confirmed the feasibility of combining the NER model [21] with semantic grouping mechanisms. Objects marked not only as named entities, but also through contextual associations (for example, mentions through pronouns, descriptive names, generalizations), were successfully associated with the corresponding propaganda techniques. This approach allowed us to avoid fragmentary analysis and provide a holistic picture of the connections between objects and rhetorical strategies.

Particular attention was paid to explaining the decisions made. The implemented LIME tools [22] provided an opportunity to illustrate which text fragments were key in determining the technique or object. An example of using local interpretation is shown in Fig. 2.

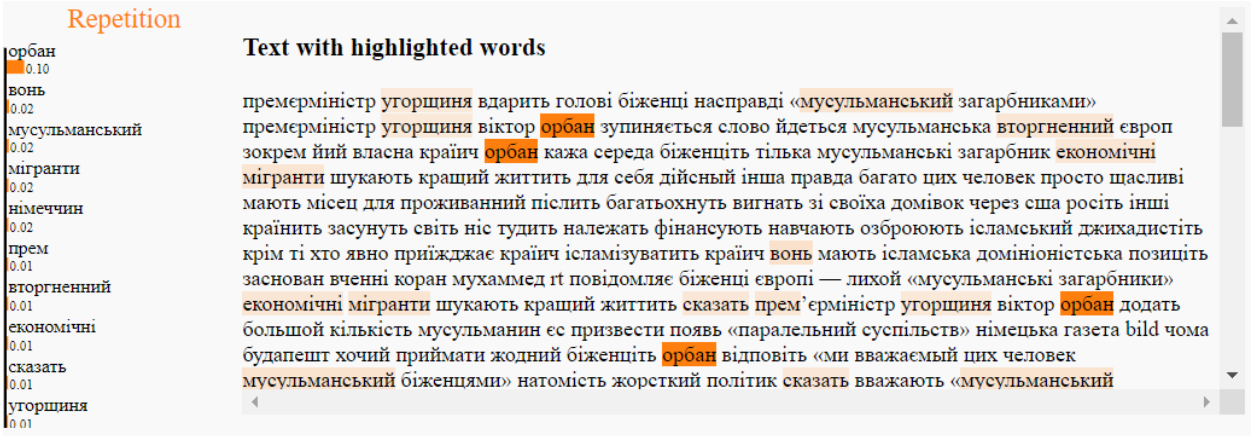


Fig.2. Using of local text interpretation

For example, in cases where the «Flag-Waving» technique was detected, tokens with high emotional modality and references to patriotic symbols gained the greatest weight, which was confirmed in LIME visualizations.

Expert evaluation of the explanations accompanying the automatic conclusions showed a high correlation between the interpretation of the model and the human perception of the influence structure. The consistency of the

results obtained automatically with the assessments of experts (Inter-Annotator Agreement at the level of 0.87) indicates the quality of not only the technical implementation, but also the ethical justification. An example of comparing the assessment of an expert with the developed software is shown in Fig.3.

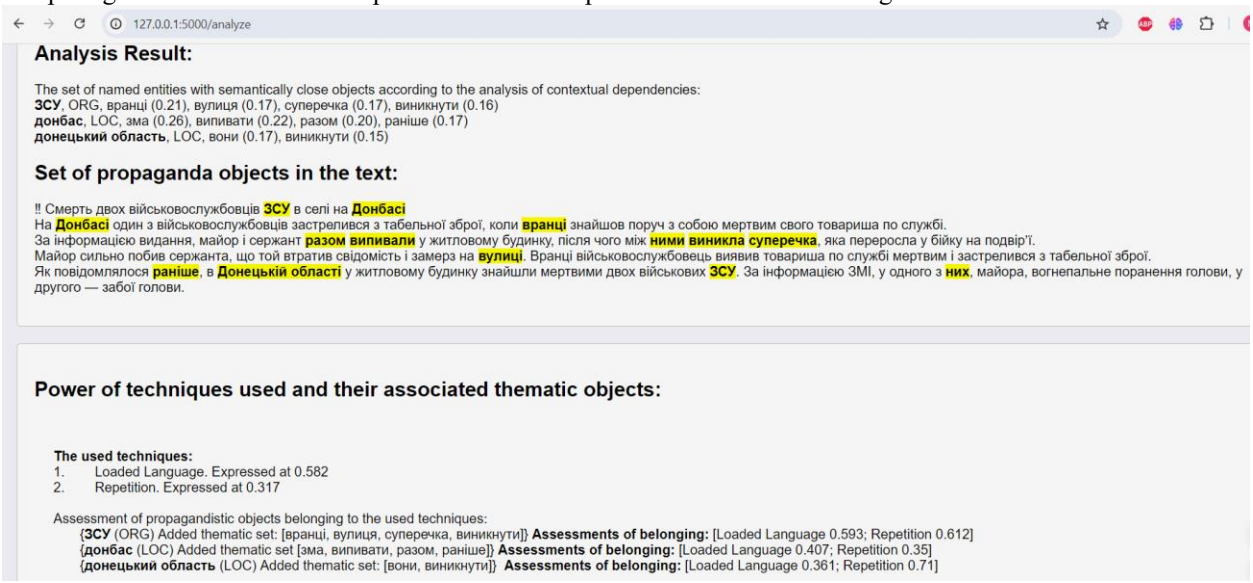


Fig. 3. An example of comparing objects and techniques of propaganda

The use of the «Charged Language» technique is used in the text to describe conflicts and violence, for example, «сильно побив», «замерз на вулиці», «застрелився з табельної зброї». This corresponds to the purpose of discrediting the Armed Forces and portraying them in a negative light, which corresponds to the expert's conclusion.

The use of the «Repetition» technique is used in the form of repeating information about the death of servicemen and violent actions. Repetition helps to enhance the negative impact and strengthen the negative impression. This corresponds to the purpose of persuading citizens not to join the ranks of the army, and active servicemen to resign.

According to the expert's conclusion (Fig.4), the theses about the alleged abuse of the Ukrainian military and the demoralization of servicemen were intended to: discredit the Armed Forces, the National Guard and other military formations in the eyes of Ukrainian citizens; convince Ukrainian citizens not to join the ranks of the Ukrainian army, and active servicemen to resign from its ranks.

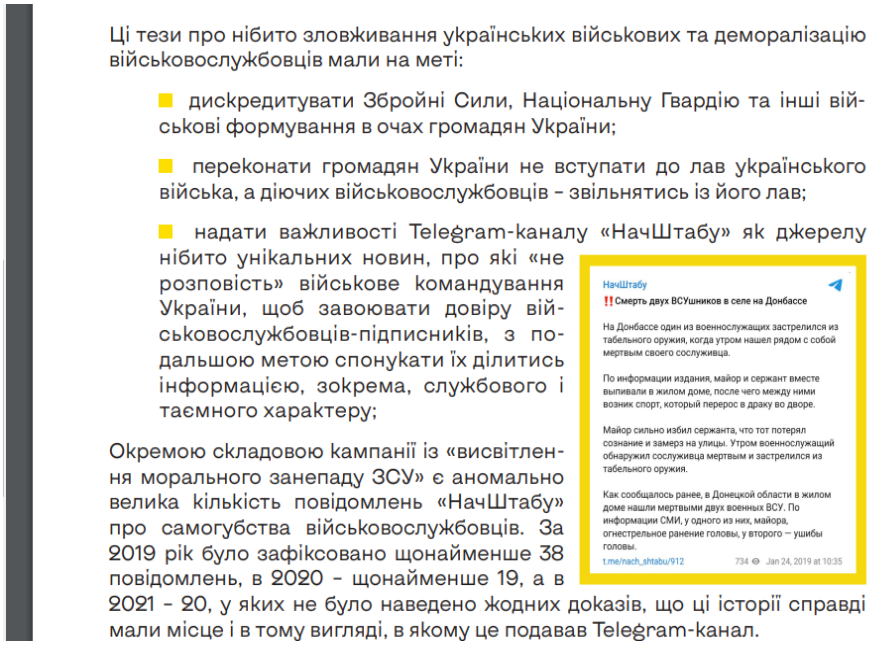


Fig. 4. Analysis of a text containing propaganda («Center of Strategic Communications» [23])

Overall, the experimental results confirm that the combination of neural network technologies with built-in transparency mechanisms allows for the creation of systems that can be used not only as an analysis tool, but also as

an object of public trust. The application of the system in real conditions – in particular, in the activities of cyber police units and public organizations – revealed its practical value both in terms of efficiency and ethical responsibility.

Conclusions

The conducted research shows that the combination of neural network technologies with methods of explainable artificial intelligent text processing allows creating an effective and at the same time ethically balanced system for detecting propaganda techniques in natural language messages. The proposed architecture provides not only high accuracy of propaganda content classification, but also demonstrates the ability to identify objects of influence and establish semantic connections between rhetorical strategies and target concepts.

The results of local interpretation and comparison with expert assessments have demonstrated the relevance and reliability of the system in the context of ethical responsibility. At the same time, the explainability of decisions, visualization of influential text fragments and transparency of computational procedures have become the basis for increasing trust in such technologies both from the user and from regulatory authorities.

In summary, it can be argued that the combination of technical efficiency with legal and ethical guarantees forms a new paradigm of responsible artificial intelligence, capable not only of detecting information threats, but also of functioning within the framework of socially acceptable and legally correct practices.

References

1. Miller K. M., Lukic K., Skiera B. The impact of the General Data Protection Regulation (GDPR) on online tracking. International Journal of Research in Marketing. 2025. URL: https://doi.org/10.1016/j.ijresmar.2025.03.002 (date of access: 05.06.2025).
2. Van Kolfschooten H., Van Oirschot J. The EU Artificial Intelligence Act (2024): Implications for healthcare. Health Policy. 2024. Vol. 149. P. 105152. URL: https://doi.org/10.1016/j.healthpol.2024.105152 (date of access: 05.06.2025).
3. Fjeld J. et al. Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI [Electronic resource] / J. Fjeld, N. Achten, H. Hilligoss, A. Nagy, M. Srikumar. – Cambridge, MA: Berkman Klein Center for Internet & Society, 2020. – 121 p. – Mode of access: https://www.abaj.ai/doc/papers/fjeld2020.pdf. – Title from screen. – Accessed: 02 June 2025.
4. UNESCO. UNESCO's Recommendation on the Ethics of Artificial Intelligence: Key Facts. – Paris: United Nations Educational, Scientific and Cultural Organization, 2023. – 16 p.
5. Kazim E., Soares Koshiyama A. Human Centric AI: A Comment on the IEEE's Ethically Aligned Design. SSRN Electronic Journal. 2020. URL: https://doi.org/10.2139/ssrn.3575140 (date of access: 06.06.2025).
6. Розпорядження Кабінету Міністрів України від 16 лютого 2024 р. № 137-р «Про затвердження плану пріоритетних дій Уряду на 2024 рік», Кабінет Міністрів України. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-priorytetnykh-dii-uriadu-na-2024-rik-137r-160224 (дата звернення: 13.03.2025).
7. SemEval-2020 Task 11: Detection of Propaganda Techniques in News Articles / G. Da San Martino et al. Proceedings of the Fourteenth Workshop on Semantic Evaluation, Barcelona (online). Stroudsburg, PA, USA, 2020. URL: https://doi.org/10.18653/v1/2020.semeval-1.186 (дата звернення: 13.04.2025).
8. Overview of the WANLP 2022 Shared Task on Propaganda Detection in Arabic / F. Alam et al. Proceedings of the The Seventh Arabic Natural Language Processing Workshop (WANLP), Abu Dhabi, United Arab Emirates (Hybrid). Stroudsburg, PA, USA, 2022. URL: https://doi.org/10.18653/v1/2022.wanlp-1.11 (дата звернення: 13.04.2025).
9. Cavaliere D., Gallo M., Stanzione C. Propaganda Detection Robustness Through Adversarial Attacks Driven by eXplainable AI. Communications in Computer and Information Science. Cham, 2023. P. 405–419. URL: https://doi.org/10.1007/978-3-031-44067-0_21 (date of access: 06.06.2025).
10. Barfar A. A linguistic/game-theoretic approach to detection/explanation of propaganda. Expert Systems with Applications. 2022. Vol. 189. P. 116069. URL: https://doi.org/10.1016/j.eswa.2021.116069 (date of access: 06.06.2025).
11. Gongane V. U., Munot M. V., Anuse A. D. A survey of explainable AI techniques for detection of fake news and hate speech on social media platforms. Journal of Computational Social Science. 2024. URL: https://doi.org/10.1007/s42001-024-00248-9 (date of access: 06.06.2025).
12. Method of Semantic Features Estimation for Political Propaganda Techniques Detection Using Transformer Neural Networks / I. Krak, M. Molchanova, V. Didur, O. Sobko, O. Mazurets, O. Barmak. CEUR Workshop Proceedings, 2025, vol. 3917, pp. 286–297. URL: https://ceur-ws.org/Vol-3917/paper56.pdf (дата звернення: 19.03.2025).
13. Method for Neural Network Detecting Propaganda Techniques by Markers With Visual Analytic / I. Krak, O. Zalutska, M. Molchanova, O. Mazurets, E. Manziuk, O. Barmak. CEUR Workshop Proceedings, 2024, vol. 3790, pp. 158–170. URL: https://ceur-ws.org/Vol-3790/paper14.pdf (дата звернення: 19.03.2025).
14. Fine-Grained Analysis of Propaganda in News Article / G. Da San Martino et al. Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), Hong Kong, China. Stroudsburg, PA, USA, 2019. URL: https://doi.org/10.18653/v1/d19-1565 (дата звернення: 13.04.2025).
15. Think Fast, Think Slow, Think Critical: Designing an Automated Propaganda Detection Tool / L. Zavolokina et al. CHI '24: CHI Conference on Human Factors in Computing Systems, Honolulu HI USA. New York, NY, USA, 2024. URL: https://doi.org/10.1145/3613904.3642805 (дата звернення: 04.12.2024).
16. Chow W. M., Levin D. H. The Diplomacy of Whataboutism and US Foreign Policy Attitudes. International Organization. 2024. Vol. 78, no. 1. P. 103–133. URL: https://doi.org/10.1017/s002081832400002x (дата звернення: 13.04.2025).
17. Молчанова М.О., Бармак О.В. Метод інтелектуального виявлення технік пропаганди за ознаками з використанням машинного навчання. Науковий журнал «Наукові праці Донецького національного технічного університету», серія «Проблеми моделювання та автоматизації проектування». 2025. №1 (21). С. 76-85. https://doi.org/10.31474/2074-7888 (дата звернення: 19.03.2025).
18. Молчанова М. Метод виявлення об'єктів пропаганди нейромережевими моделями глибокого навчання з візуальною інтерпретацією прийнятих рішень. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. 2024. Т. 343, № 6(1). С. 179–185. URL: https://doi.org/10.31891/2307-5732-2024-343-6-27 (дата звернення: 19.03.2025).
19. Merryton A. R., Gethsiyal Augasta M. An Attribute-wise Attention model with BiLSTM for an efficient Fake News Detection. Multimedia Tools and Applications. 2023. URL: https://doi.org/10.1007/s11042-023-16824-6 (дата звернення: 02.04.2025).
20. Large Language Models: Comparing Gen 1 Models (GPT, BERT, T5 and More). Dev. URL: https://dev.to/admantium/large-language-models-comparing-gen-1-models-gpt-bert-t5-and-more-74h (дата звернення: 13.03.2025).
21. Wilkho R. S., Gharaibeh N. G. FF-NER: A named entity recognition model for harvesting web-based information about

flash floods and related infrastructure impacts. International Journal of Disaster Risk Reduction. 2025. Vol. 125. P. 105604. URL: https://doi.org/10.1016/j.ijdrr.2025.105604 (date of access: 06.06.2025).

22. ELI5.LIME: Explain PyTorch Text Classification Network Predictions Using LIME Algorithm, CoderzColumn, 2024. URL: https://coderzcolumn.com/tutorials/artificial-intelligence/eli5-lime-explain-pytorch-text-classification-network-predictions (дата звернення: 06.04.2025).

23. Центр стратегічних комунікацій, Spravdi, 2025. URL: https://spravdi.gov.ua/ (дата звернення: 06.04.2025).

Maryna Molchanova **Марина Молчанова**	Postgraduate student, Department of Computer Science, Khmelnytskyi National University https://orcid.org/0000-0001-9810-936X e-mail: m.o.molchanova@gmail.com	Аспірант кафедри комп'ютерних наук, Хмельницький національний університет
Pawan Kumar Dutt **Паван Кумар Датт**	Doctor of Philosophy, Senior Lecturer at the School of Law, Tallinn University of Technology (Estonia). https://orcid.org/0000-0001-8772-0315	Доктор філософії, старший викладач Школи права Талліннського технічного університету (Естонія).

https://doi.org/10.31891/csit-2025-2-12

UDC 004.41+004.43:519.6

Oleg ZHULKOVSKYI
Dniprovsky State Technical University
Inna ZHULKOVSKA
University of Customs and Finance
Hlib VOKHMIANIN
Dniprovsky State Technical University
Anastasiia TKACH
Dniprovsky State Technical University

COMPARATIVE ANALYSIS OF COMPUTATIONAL PERFORMANCE OF MODERN PROGRAMMING LANGUAGES

The study is dedicated to the comparative analysis of the computational performance of modern programming languages in the implementation of numerical methods for solving boundary value problems in mathematical physics. The central focus of the research is the Thomas algorithm – an efficient numerical method for solving systems of linear algebraic equations with a tridiagonal matrix. The research methodology is based on a unified implementation of the Thomas algorithm for each examined programming language, ensuring identical algorithmic logic. Experimental testing was conducted on systems with sizes ranging from 10^5 to 1.5×10^7 elements for programming languages including C, C++, C#, Java, JavaScript, Go, and Python, which represent different paradigms and approaches to computation. The obtained results demonstrate significant differences in the performance of various programming languages. It was established that low-level compiled languages exhibit the highest execution speed, especially for large problem sizes. In contrast, interpreted languages show significantly lower performance, which becomes more pronounced as the computational workload increases.

The study experimentally confirmed the impact of compiler optimization modes on performance, revealing differences of up to 70% depending on the language and optimization level. The scientific novelty of this work lies in the comprehensive investigation of programming language performance in the context of numerical modeling by comparing their characteristics when solving mathematical problems. Future research will include an in-depth study of the impact of processor architecture, compiler optimization mechanisms, and runtime environment implementation on the performance of computational algorithms, as well as an expansion of the range of numerical methods and programming languages analyzed.

Keywords: programming language performance, SLAE, Thomas algorithm, optimization levels.

Олег ЖУЛЬКОВСЬКИЙ
Дніпровський державний технічний університет
Інна ЖУЛЬКОВСЬКА
Університет митної справи та фінансів, м. Дніпро
Гліб ВОХМЯНІН
Дніпровський державний технічний університет
Анастасія ТКАЧ
Дніпровський державний технічний університет

ПОРІВНЯЛЬНИЙ АНАЛІЗ ОБЧИСЛЮВАЛЬНОЇ ШВИДКОДІЇ СУЧАСНИХ МОВ ПРОГРАМУВАННЯ

Дослідження присвячене порівняльному аналізу обчислювальної швидкодії сучасних мов програмування при реалізації чисельних методів розв'язання крайових задач математичної фізики. Центральним об'єктом дослідження виступає метод прогонки – ефективний чисельний алгоритм розв'язання систем лінійних алгебраїчних рівнянь з тридіагональною матрицею. Методологія дослідження базується на уніфікованій реалізації методу прогонки для кожної досліджуваної мови з ідентичною алгоритмічною логікою. Експериментальні випробування проведено на системах розмірністю від 10^5 до $1,5 \times 10^7$ елементів для мов програмування C, C++, C#, Java, JavaScript, Go, Python, які репрезентують різні парадигми та підходи до виконання обчислень. Отримані результати демонструють суттєві відмінності у продуктивності різних мов програмування. Встановлено, що компільовані мови низького рівня демонструють найвищу швидкодію, особливо при великих розмірностях задач. Натомість інтерпретовані мови мають значно нижчу продуктивність, що відстежується при збільшенні обсягу обчислень. Експериментально підтверджено вплив оптимізаційних режимів компіляції на продуктивність, демонструючи різницю до 70% залежно від мови та рівня оптимізації. Наукова новизна роботи полягає в комплексному дослідженні продуктивності різних мов програмування в контексті чисельного моделювання шляхом порівняння їхніх характеристик при розв'язанні математичних задач. Подальші дослідження включають поглиблене вивчення впливу архітектури процесора, механізмів оптимізації компіляторів та особливостей реалізації середовищ виконання на продуктивність обчислювальних алгоритмів, а також розширення спектру досліджуваних чисельних методів та мов програмування.

Ключові слова: швидкодія мови програмування, СЛАР, метод прогонки, рівні оптимізації.

Introduction

In the context of rapid development of software and computing technology, the issue of intensifying computational processes is becoming increasingly relevant, as the speed of algorithm execution directly affects data processing efficiency and system performance [1]. The diversity of modern systems and programming languages,

their interaction with hardware resources, memory management, compilation processes, and other factors highlight the importance of selecting an appropriate language for solving computational problems. A particularly critical criterion in choosing a programming language for computational modeling tasks is the execution speed of programs. Thus, researchers face the question of which programming language is the most effective for implementing numerical algorithms used in computer models.

In computational modeling tasks that ultimately reduce to the numerical solution of systems of linear algebraic equations (SLAE) with a tridiagonal matrix, the Tri-Diagonal Matrix Algorithm (TDMA) is frequently used. TDMA is specifically applied to solving SLAEs arising from the discretization of differential equations using the finite difference or finite element methods for boundary value problems. It is one of the most efficient algorithms, ensuring SLAE solutions in linear time [2].

Despite its algorithmic efficiency, the practical performance of TDMA can vary significantly depending on the programming language used for its implementation.

The aim of this study is to identify the most efficient programming languages in terms of execution speed for the TDMA implementation. For comparative analysis, the study will examine modern high-ranking [3] programming languages: C, C++, C#, Python, Java, JavaScript, and Go.

Related works

The performance of computational processes is determined not only by the specifics of their algorithmic implementation but also by other factors, including the choice of programming language. Programming languages differ in their paradigms, memory management mechanisms, levels of abstraction, and execution models, all of which directly impact the speed and resource efficiency of implemented algorithms [1, 4]. The relationship between programming languages and execution efficiency becomes increasingly significant given the continuous growth of data volumes that require complex processing. The evolution of computing architectures, including multi-core processors, graphics accelerators, and specialized computational devices [5], adds an additional layer of complexity, as different languages exhibit varying degrees of efficiency in hardware optimization. Consequently, the same algorithm, when implemented in different programming languages, may exhibit different execution times.

For example, the discrete wavelet transform (DWT) method for audio signal analysis demonstrates varying execution times when implemented in different programming languages [1]. The results highlight the advantages and superior performance of C and C++ in digital signal processing tasks.

In another context, a comparison of PHP, Python, Node.js, and Golang for API development in cloud environments has shown [4] that Golang provides the best scalability and performance under high loads, whereas Node.js performs well in systems with medium workloads.

Reference [6] presents a performance analysis of JSON parsers in Java, Python, C#, JavaScript, and PHP, examining their efficiency in terms of parsing speed and resource consumption within their respective native environments. The evaluation was conducted using JSON test files with varying levels of nesting and data volumes. The study utilized monitoring tools on the Windows 10 operating system to analyze performance, enabling the identification of language-specific parser implementations in the context of semi-structured data processing.

Interpreted languages such as Python offer greater flexibility and faster development cycles, thereby improving developer productivity. Although interpreted languages are generally slower than compiled ones [7], advancements such as just-in-time (JIT) compilers and transpilers have significantly narrowed this performance gap [8]. A study comparing three compiled languages – Fortran, C++, and Java – and three interpreted languages – Python, MATLAB, and Julia – was conducted based on their popularity and technical advantages. These six languages were evaluated and compared in terms of capabilities, performance, and ease of use through the implementation of idiomatic solutions to classical astrodynamics problems. The results confirmed that compiled languages still provide the highest execution performance, but JIT-compiled dynamic languages have achieved competitive speed levels and offer an attractive trade-off between numerical efficiency and developer productivity.

A comparative analysis of Python and Scala for big data processing was conducted using Apache Spark – an open-source in-memory cluster computing system designed for high-speed processing [9]. The study concluded that both languages are suitable for Apache Spark, but the choice depends on project-specific requirements, balancing development convenience, performance, and data integration efficiency.

Reference [10] also compares the performance of Scala and Java in the Apache Spark MLlib environment through a series of tests involving various machine learning methods. The experiments demonstrated that Scala outperforms Java by 10–20% in performance, depending on the algorithm's characteristics.

Reference [11] analyzes the performance of C, Python, MATLAB, and LabVIEW in instrumentation automation tasks. The results indicate that C exhibits minimal resource consumption and optimal performance for small data volumes, whereas Python is advantageous for interface setup and efficient memory usage. MATLAB delivers the fastest processing for large datasets, while LabVIEW surpasses other tools in real-time control tasks and maintains stable performance in graphical rendering. Similar to the findings in [9], language selection depends on task-specific requirements – C is optimal for resource-constrained systems, MATLAB is suited for complex computations, LabVIEW is ideal for real-time control, and Python excels in multi-device integration.

A systematic review of WebAssembly (WASM) and JavaScript performance in various aspects (execution time, memory usage, and energy consumption) demonstrated [12] that WASM is more efficient in lightweight applications due to its faster execution and lower energy consumption. However, in more complex applications, JavaScript exhibits lower resource consumption and higher execution speed.

A comparative performance analysis of MicroPython (a Python implementation in C for microcontrollers) and C was conducted on STM32 and ESP32 microcontrollers [13]. The study evaluated memory allocation speed and the execution efficiency of cryptographic algorithms such as SHA-256 and CRC-32. The results indicated that despite certain limitations, MicroPython can be an effective tool for low-cost microcontrollers when appropriate optimizations are applied.

Reference [14] further examines the performance of C/C++, MicroPython, Rust, and TinyGo on the ESP32 microcontroller in IoT applications. The study focused on data and signal processing algorithm execution speed, as well as development convenience. The results revealed the advantages and limitations of each language depending on specific requirements and application scenarios. Implementations in C/C++ were the fastest in most cases, followed by TinyGo and Rust, while MicroPython applications were significantly slower. Thus, C/C++, TinyGo, and Rust are better suited for scenarios where execution time and response time are critical, whereas Python offers a faster and less complex development process for less stringent system requirements.

A comparative analysis of Go, Java, and Python in decision-support processes for Industry 4.0 was conducted in [15]. The study examined decision tree algorithms based on entropy heuristics, evaluating parameters such as memory usage, CPU utilization, and computation time to determine the suitability of these languages for industrial solutions in the Industry 4.0 framework.

Programming languages may exhibit different execution times for algorithms implemented synchronously, asynchronously, or in parallel. In parallel metaheuristics commonly used for solving NP-hard optimization problems, a comparison of Chapel, Julia, and Python demonstrated [16] that none of these languages outperform C combined with OpenMP in performance. However, they offer a trade-off between execution speed and development convenience.

Reference [17] compares structured approaches to parallelism in Java and Kotlin, analyzing their performance, real-world adaptability, and optimization capabilities for multi-threaded applications. Both languages operate on the Java Virtual Machine (JVM), inherently supporting traditional thread-based concurrency. However, Kotlin includes lightweight coroutines for parallelism, whereas Java's virtual threads, introduced in Project Loom, remain experimental. A review of recent scientific studies highlights the multifactorial dependence of computational performance on programming language choice, driven by differences in paradigms, memory management mechanisms, abstraction levels, and execution models. Studies demonstrate that lower-level languages, such as C and C++, provide the highest efficiency in digital signal processing and resource-constrained systems. For web development and API performance, efficiency varies – Golang offers optimal scalability under high loads, while Node.js is a suitable choice for medium workloads. In big data processing, the choice between Python and Scala for Apache Spark depends on the balance between development convenience and integration efficiency. Comparative studies of WebAssembly and JavaScript reveal context-dependent efficiency: WASM performs better in simple applications, while JavaScript excels in more complex ones. In microcontroller-based systems, C/C++, TinyGo, and Rust confirm their advantages in execution time and response speed, whereas MicroPython provides a trade-off between development speed and efficiency.

A review of recent scientific studies highlights the multifactorial dependence of computational performance on programming language choice, driven by differences in paradigms, memory management mechanisms, abstraction levels, and execution models. Studies demonstrate that lower-level languages, such as C and C++, provide the highest efficiency in digital signal processing and resource-constrained systems. For web development and API performance, efficiency varies – Golang offers optimal scalability under high loads, while Node.js is a suitable choice for medium workloads. In big data processing, the choice between Python and Scala for Apache Spark depends on the balance between development convenience and integration efficiency. Comparative studies of WebAssembly and JavaScript reveal context-dependent efficiency: WASM performs better in simple applications, while JavaScript excels in more complex ones. In microcontroller-based systems, C/C++, TinyGo, and Rust confirm their advantages in execution time and response speed, whereas MicroPython provides a trade-off between development speed and efficiency. Parallel computing support is also a significant factor affecting performance. Traditional C with OpenMP [18] retains its dominant position over higher-level but more developer-friendly languages such as Chapel, Julia, and Python.

In the context of Industry 4.0 and decision-support systems, key selection criteria for programming languages include memory usage, CPU utilization, and computational time. Differences in parallelism models also contribute to performance variability. Thus, selecting a programming language for a specific task should be based on a comprehensive analysis of execution efficiency, development convenience, and application-specific requirements, as supported by systematic empirical research.

To achieve the research objective, this study aims to perform a comparative analysis of the computational efficiency of TDMA implementations using the prominent programming languages C, C++, C#, Python, Java, JavaScript, and Go.

Materials and Methods

For conducting a comparative analysis of the computational efficiency of different programming languages, TDMA was chosen, as described in [19].

The mathematical model of the problem for numerically solving a system of n linear algebraic equations is as follows:

$$a_i x_{i-1} - c_i x_i + b_i x_{i+1} = -f_i,$$
$$a_i \neq 0, b_i \neq 0, i = 1...n;$$
$$a_1 = 0, b_n = 0;$$
$$|c_1| \geq |b_1|;$$
$$|c_n| \geq |a_n|;$$
$$|c_i| > |a_i| + |b_i|, i = 2...n-1,$$

where the last three inequalities represent the diagonal dominance conditions, ensuring the numerical stability of the method.

The pseudocode for the TDMA solution of a tridiagonal system of linear algebraic equations using the Double Sweep Method can be presented as follows:

TDMA: pseudo code (Double Sweep Method)

```
1.  p = n / 2
2.  // forward pass
3.  For i = 1 to p do // right sweep
4.     den = c[i] - a[i] * alfa[i]
5.     alfa[i+1] = b[i] / den
6.     beta[i+1] = (a[i] * beta[i] + f[i]) / den
7.  End for
8.
9.  For i = n downto p do // left sweep
10.    den = c[i] - b[i] * ksi[i+1]
11.    ksi[i] = a[i] / den
12.    eta[i] = (b[i] * eta[i+1] + f[i]) / den
13. End for
14.
15. // conjugation of solutions
16. x[p] = (alfa[p+1] * eta[p+1] + beta[p+1]) / (1 – alfa[p+1] * ksi[p+1])
17.
18. // backward pass
19. For i = p-1 downto 1 do // right sweep
20.    x[i-1] = alfa[i+1] * x[i+1] + beta[i+1]
21. End for
22.
23. For i = p to n-1 do // left sweep
24.    x[i+1] = ksi[i+1] * x[i] + eta[i+1]
25. End for
```

At the beginning of the algorithm (line 1), the splitting point p is set, dividing the system of dimension n in half. In lines 3–7, the forward sweep of the right pass is performed to compute the sweep coefficients α, β for the first half of the system. In lines 9–13, the forward sweep of the left pass is executed to compute the sweep coefficients ξ, η for the second half of the system, respectively. The reconciliation of both solution parts at point p is implemented in line 16. After coupling, the backward sweeps are performed: in lines 19–21 for the right pass and in lines 23–25 for the left pass, respectively.

Experiments

All experiments were conducted on a single computer with the following specifications:

– CPU: AMD Ryzen 5 350OU, 2100 MHz, 4 cores, 8 threads;

– RAM: Goodram DDR4 (4 GB, 2666 MHz) × 2 = 8 GB;

– OS: Microsoft Windows 11 Pro.

The experiments were conducted for the system size n=10^5–1.5×10^7.

Seven programming languages were chosen for the study, representing different programming paradigms and approaches to compilation and interpretation (Table 1).

Table 1

Characteristics of the studied programming languages

Language	Classification	Typing	Brief description
C	Compiled	Static	A mid-level language with a minimal level of abstraction. Implemented using the standard GCC compiler [20].
C++	Compiled	Static	A language with support for object-oriented and generic programming. Implemented using the standard G++ compiler [20].
C#	Compiled	Static	A language for the .NET platform, using intermediate code (IL) and a virtual machine (CLR) [21].
Java	Compiled-Interpreted	Static	An object-oriented programming language that uses bytecode, executed by the Java Virtual Machine (JVM) [22].
JavaScript (JS)	Interpreted	Dynamic	A multi-paradigm language, implemented using various engines, including Node.js for server-side execution [23].
Python	Interpreted	Dynamic	A multi-paradigm language, implemented with the standard CPython interpreter [24].
Golang (Go)	Compiled	Static	A language with built-in support for concurrent programming and fast compilation. Developed to improve development productivity [25].

The methodology for measuring execution time is adapted to the specifics of each programming language using the following approaches:

– The clock() function from the time.h library for the C language [20];
– The use of std::chrono::steady_clock for high-precision measurement in C++ [20];
– The application of the Stopwatch class from the System.Diagnostics namespace in C# [21];
– Measurement using System.nanoTime() in Java [22];
– The performance.now() function from the high-precision time measurement API in JavaScript [23];
– The time.perf_counter() function, providing the highest available resolution in Python [24];
– The time.Now() function and duration measurement methods in Go [25].

During the experiments, only the execution time of the algorithmic part of the program was measured, excluding the time for initializing the execution environment, loading the interpreter, or allocating memory for the initial data structures.

Compilation and execution of the programs were performed using the built-in optimization features of each programming language.

To investigate the impact of built-in optimization efficiency, additional experiments were conducted for C-like languages in Debug x64 mode (no optimization, -Od) and Release x64 mode (optimization with a focus on execution speed, -O2).

Results

The obtained results are summarized in Table 2 and Table 3 and presented as graphs showing the relationship between execution time and the system size for different programming languages (Fig. 1–3).

Table 2

Results of computational experiments for Python, Java, JavaScript, and Go with built-in optimization

SLAE order	Computation time, s			
	Python	Java	JavaScript	Go
1×10^5	0.1030	0.0193	0.0207	0.0020
2×10^5	0.2064	0.0258	0.0239	0.0050
3×10^5	0.3278	0.0357	0.0330	0.0070
4×10^5	0.4283	0.0359	0.0427	0.0098
5×10^5	0.4607	0.0386	0.0430	0.0118
6×10^5	0.5906	0.0396	0.0520	0.0142
7×10^5	0.7272	0.0416	0.0488	0.0180
8×10^5	0.8575	0.0490	0.0547	0.0208
9×10^5	0.9914	0.0479	0.0609	0.0244
1×10^6	1.2253	0.0490	0.0653	0.0280
2.5×10^6	2.8130	0.0850	0.1563	0.0589
5×10^6	5.6513	0.1397	0.3152	0.1202
1×10^7	10.2515	0.2786	0.6183	0.2498
1.5×10^7	14.9313	0.4496	0.9861	0.4055

The comparative analysis of interpreted languages (Python, JavaScript) and compiled languages (Java, Go, C, C++, C#) revealed a nonlinear dependence of execution time on system size, which follows an exponential pattern (Fig. 2). For Python and JavaScript, there is significantly higher sensitivity to the increase in system size. Specifically, when transitioning from a system size of 10^5 to 10^7 the execution time for Python increases approximately 145 times (from 0.103 s to 14.9313 s), and for JavaScript, it increases more than 30 times (from 0.0207 s to 0.9861 s).

On the other hand, compiled languages show a fundamentally different pattern. Go demonstrates almost a linear relationship between execution time and system size. C and C++ exhibit similar results with minimal

execution time overhead. Notably, for the maximum system size of 1.5×10^7 Python requires nearly 15 seconds of computation, whereas Go takes only 0.4055 seconds, Java 0.4496 seconds, and C++ about 0.3637 seconds (Fig. 3).

Table 3

Results of computational experiments for C-like languages in different optimization modes

SLAE order	Computation time, s					
	C (-Od)	C (-O2)	C++ (-Od)	C++ (-O2)	C# (-Od)	C# (-O2)
1×10^5	0.0010	0.0010	0.0023	0.0030	0.0050	0.0040
2×10^5	0.0050	0.0030	0.0062	0.0045	0.0116	0.0067
3×10^5	0.0080	0.0060	0.0073	0.0056	0.0143	0.0088
4×10^5	0.0110	0.0060	0.0106	0.0115	0.0191	0.0115
5×10^5	0.0150	0.0090	0.0162	0.0140	0.0223	0.0165
6×10^5	0.0320	0.0090	0.0179	0.0189	0.0339	0.0183
7×10^5	0.0190	0.0140	0.0212	0.0211	0.0399	0.0203
8×10^5	0.0250	0.0140	0.0245	0.0246	0.0406	0.0220
9×10^5	0.0260	0.0180	0.0279	0.0277	0.0443	0.0266
1×10^6	0.0290	0.0150	0.0373	0.0293	0.0533	0.0314
2.5×10^6	0.0670	0.0420	0.0631	0.0632	0.1432	0.0770
5×10^6	0.1170	0.0780	0.1213	0.1113	0.2553	0.1684
1×10^7	0.2750	0.1730	0.2904	0.2250	0.4836	0.4054
1.5×10^7	0.5150	0.2950	0.4836	0.3637	0.7947	0.7006

For C-like languages, the transition from the non-optimized mode (-Od) to the optimized mode (-O2) demonstrates a performance boost of approximately 1.15x for C#, 1.3x for C++, and from 1.5x to 1.7x for C.

Go shows the greatest stability in performance as the problem size increases. Execution time increases almost proportionally to the increase in system size. Java and C# occupy an intermediate position, demonstrating fairly high efficiency due to Just-In-Time (JIT) compilation and advanced runtime optimization mechanisms.

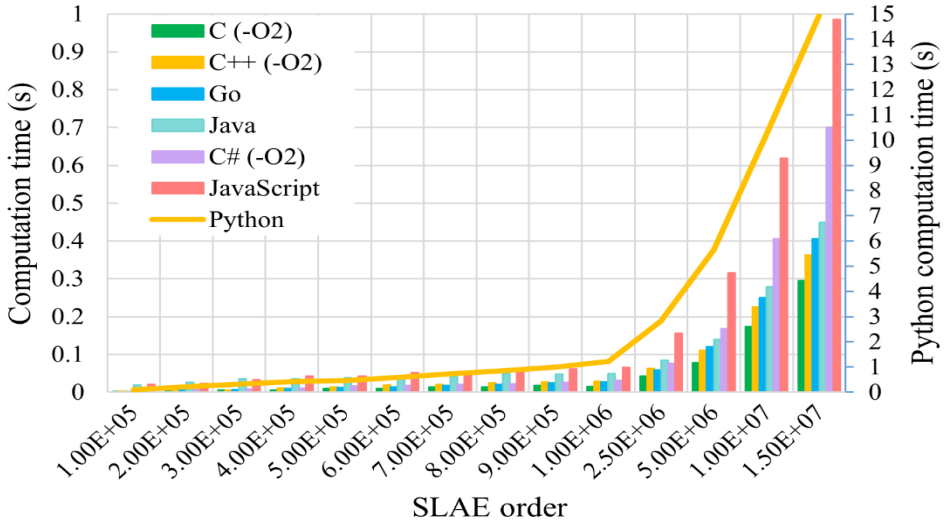


Fig. 1. General results of computational experiments

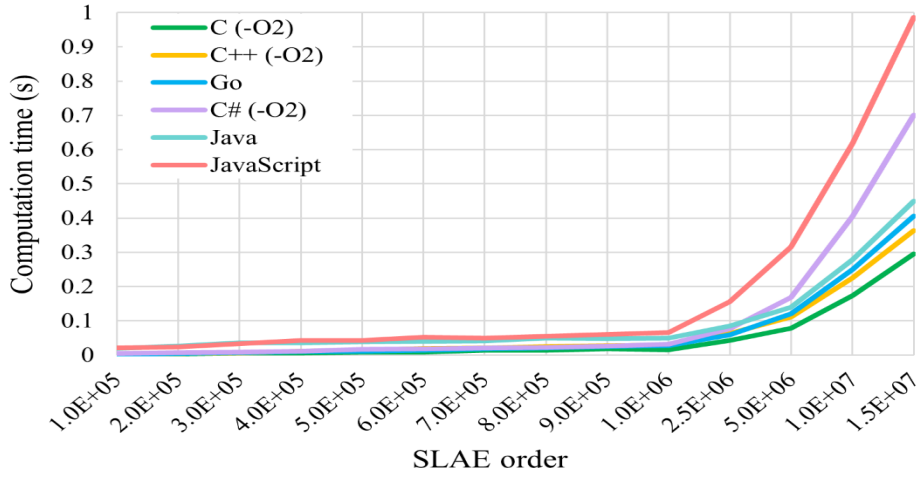


Fig. 2. Results of computational experiments for C-like languages, Java, JavaScript, and Go

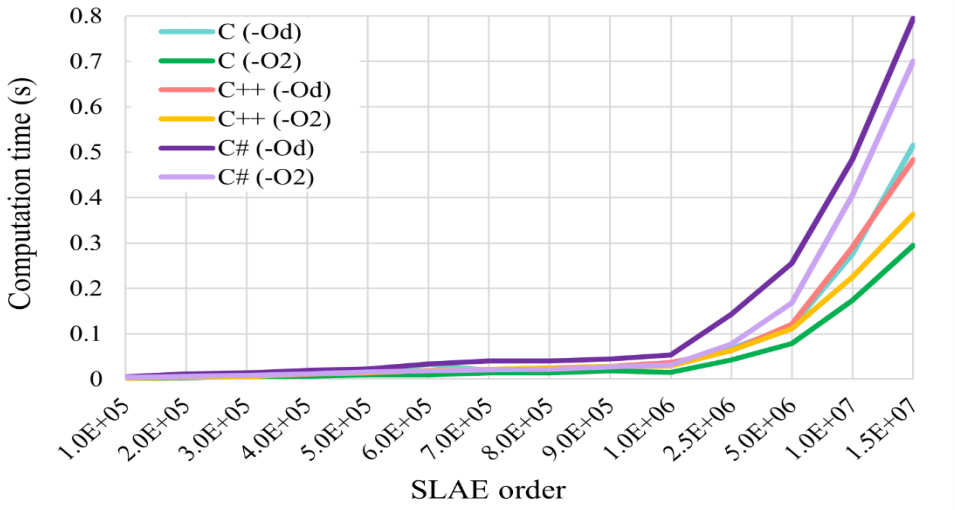


Fig. 3. Comparison of results in different optimization modes for C-like languages

The conducted experiments prove that for high-performance scientific computing, especially in computer simulation, compiled languages with explicit static typing, such as Go, C/C++, and Java, are the most effective, as they provide minimal overhead and high scalability of computational algorithms.

Conclusions

The conducted study presents a comprehensive analysis of the computational efficiency of modern programming languages in implementing numerical methods of mathematical physics, specifically the TDMA for solving SLAE with tridiagonal matrices.

The scientific novelty of this work lies in a systematic comparative study of the performance of various programming languages using a unified methodology for experimental research. This approach enables an objective quantitative assessment of the computational performance of modern languages in solving typical numerical mathematics problems.

Compiled languages, particularly C/C++, Go, and Java, demonstrated the highest performance and the lowest sensitivity to increasing problem size. In contrast, interpreted languages such as Python and JavaScript exhibited significantly lower computational efficiency, characterized by an exponential increase in execution time as the problem size grows. However, their advantage lies in the simplicity of development and rapid prototyping.

The transition from an unoptimized compilation mode to a fully optimized mode results in a speedup of approximately 1.15x for C#, 1.3x for C++, and between 1.5x and 1.7x for C, confirming the necessity of proper compiler configuration to achieve optimal computational performance. Meanwhile, the Go programming language demonstrated the highest stability in performance when scaling computational tasks. Go's uniqueness lies in its combination of high execution speed, a relatively simple syntax, and built-in concurrency mechanisms.

A comparative analysis of C and C++ confirmed that these languages remain the most efficient for low-level computations, ensuring minimal overhead and a close-to-hardware implementation of algorithms. This conclusion aligns with the findings of previous research [1, 8, 11].

Future research directions include an in-depth study of the impact of computer system architecture, compiler optimization mechanisms, and runtime environment characteristics on the performance of computational algorithms. Additionally, expanding the range of numerical methods and programming languages under investigation will provide further insights into computational efficiency across different paradigms.

References

1. J. P. L. Escola, U. B. d. Souza, L. d. C. Brito. Discrete Wavelet Transform in digital audio signal processing: A case study of programming languages performance analysis. *Comput. Elect. Eng.* 2022. Vol. 104. DOI: https://doi.org/10.1016/j.compeleceng.2022.108439

2. N. D. Katopodes. Basic Concepts. *Free-Surface Flow*. 2019. P. 2–79. DOI: https://doi.org/10.1016/b978-0-12-815485-4.00007-3

3. TIOBE Index. URL: https://www.tiobe.com/tiobe-index (date of access: 15.03.2025).

4. T. Tanadechopon, B. Kasemsontitum. Performance Evaluation of Programming Languages as API Services for Cloud Environments: A Comparative Study of PHP, Python, Node.js and Golang. *2023 7th Int. Conf. Inf. Technol (InCIT)*. Chiang Rai, 16–17 Nov., 2023. P. 17–21. DOI: https://doi.org/10.1109/incit60207.2023.10413079

5. J. L. Hennessy, D. A. Patterson. A new golden age for computer architecture. *Commun. ACM*. 2019. Vol. 62, No. 2. P. 48–60. DOI: https://doi.org/10.1145/3282307

6. H. K. Dhalla. A Performance Analysis of Native JSON Parsers in Java, Python, MS.NET Core, JavaScript, and PHP. *2020 16th Int. Conf. Netw. Service Manage. (CNSM)*, Izmir, 2–6 Nov. 2020. P. 1–5. DOI: https://doi.org/10.23919/cnsm50824.2020.9269101

7. I. I. Zhulkovska, O. O Zhulkovskyi, V. V. Bilio. Typizatsiia suchasnykh mov prohramuvannia: zbirnyk naukovykh prats DDTU. *Tekhnichni nauky*. 2017. Vol. 30, No. 1. P. 154–158.

8. H. Eichhorn, R. Angerl, J. L. Cano, F. McLean. A Comparative Study of Programming Languages for Next-Generation Astrodynamics Systems. *6th International Conference on Astrodynamics Tools and TechniquesAt*. Darmstadt, March 2016. URL:

https://www.researchgate.net/publication/298577453_A_Comparative_Study_of_Programming_Languages_for_Next-Generation_Astrodynamics_Systems

9. Y. K. Gupta, S. Kumari. A Study of Big Data Analytics using Apache Spark with Python and Scala. *3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, Thoothukudi, 3–5 Dec. 2020. P. 471–478. DOI: https://doi.org/10.1109/iciss49785.2020.9315863

10. H. K. Omar, A. K. Jumaa. Big Data Analysis Using Apache Spark MLlib and Hadoop HDFS with Scala and Java. *Kurdistan J. Appl. Res.* 2019. Vol. 4, No. 1. P. 7–14. DOI: https://doi.org/10.24017/science.2019.1.2

11. A. Kumar, M. Goswami. Performance comparison of instrument automation pipelines using different programming languages. *Scientific Rep.* 2023. Vol. 13, No. 1. DOI: https://doi.org/10.1038/s41598-023-45849-y

12. J. W. Sunarto, A. Quincy, F. S. Maheswari, Q. D. A. Hafizh, M. G. Tjandrasubrata, M. H. Widianto. A Systematic Review of WebAssembly VS Javascript Performance Comparison. *Int. Conf. Inf. Manage. Technol. (ICIMTech)*. Malang, 24–25 Aug. 2023. P. 241–246. DOI: https://doi.org/10.1109/icimtech59029.2023.10277917

13. V. M. Ionescu, F. M. Enescu. Investigating the performance of MicroPython and C on ESP32 and STM32 microcontrollers. *2020 IEEE 26th Int. Symp. Des. Technol. Electron. Packag. (SIITME)*. Pitesti, 21–24 Oct. 2020. P. 234–237. DOI: https://doi.org/10.1109/siitme50350.2020.9292199

14. I. Plauska, A. Liutkevičius, A. Janavičiūtė. Performance Evaluation of C/C++, MicroPython, Rust and TinyGo Programming Languages on ESP32 Microcontroller. *Electronics*. 2022. Vol. 12, No. 1. P. 143. DOI: https://doi.org/10.3390/electronics12010143

15. P. Dymora, A. Paszkiewicz. Performance Analysis of Selected Programming Languages in the Context of Supporting Decision-Making Processes for Industry 4.0. *Appl. Sci*. 2020. Vol. 10, No. 23. P. 8521. DOI: https://doi.org/10.3390/app10238521

16. J. Gmys, T. Carneiro, N. Melab, E.-G. Talbi, D. Tuyttens. A comparative study of high-productivity high-performance programming languages for parallel metaheuristics. *Swarm Evol. Computation*. 2020. Vol. 57. DOI: https://doi.org/10.1016/j.swevo.2020.100720

17. D. Beronic, L. Modric, B. Mihaljevic, A. Radovan. Comparison of Structured Concurrency Constructs in Java and Kotlin – Virtual Threads and Coroutines. *2022 45th Jubilee Int. Conv. Inf., Communication Electron. Technol. (MIPRO)*. Opatija, 23–27 May 2022. P. 1466–1471. DOI: https://doi.org/10.23919/mipro55190.2022.9803765

18. O. O. Zhulkovskyi, I. I. Zhulkovska, V. V. Shevchenko. Evaluating the effectiveness of the implementation of computational algorithms using the OpenMP standard for parallelizing programs, *Inform. math. methods simul*. 2021. Vol. 11, No. 4. P. 268–277. DOI: https://doi.org/10.15276/imms.v11.no4.268

19. O. Zhulkovskyi, I. Zhulkovska, P. Kurliak, O. Sadovoi, Y. Ulianovska, H. Vokhmianin. Using asynchronous programming to improve computer simulation performance in energy systems. *Energetika*. 2025. Vol. 71, No. 1. P. 23–33. DOI: https://doi.org/10.6001/energetika.2025.71.1.2

20. C\C++ Documentation. URL: https://learn.microsoft.com/en-us/cpp (date of access: 15.03.2025).

21. C# and .NET Documentation. URL: https://learn.microsoft.com/en-us/dotnet (date of access: 15.03.2025).

22. Java Documentation. URL: https://docs.oracle.com/en/java (date of access: 15.03.2025).

23. JavaScript: Node.js Documentation. URL: https://nodejs.org/docs/latest/api (date of access: 15.03.2025).

24. Python 3 Documentation. URL: https://docs.python.org/3 (date of access: 15.03.2025).

25. Go Documentation. URL: https://go.dev/doc (date of access: 15.03.2025).

Oleg Zhulkovskyi **Олег Жульковський**	PhD, Associate Professor, Acting Head of the Department of Software Systems, Dniprovsky State Technical University https://orcid.org/0000-0003-0910-1150 e-mail: olalzh@ukr.net	Кандидат технічних наук, в.о. завідувача кафедри програмного забезпечення систем, Дніпровський державний технічний університет
Inna Zhulkovska **Інна Жульковська**	PhD, Associate Professor of Department of Cybersecurity and Information Technologies, University of Customs and Finance https://orcid.org/0000-0002-6462-4299 e-mail: inivzh@gmail.com	Кандидат технічних наук, доцент кафедри кібербезпеки та інформаційних технологій, Університет митної справи та фінансів, м.Дніпро
Hlib Vokhmianin **Гліб Вохмянін**	Master Student of the Department of Software Systems, Dniprovsky State Technical University https://orcid.org/0000-0002-9582-5990 e-mail: vohmyanin.yleb@gmail.com	Здобувач вищої освіти другого (магістерського) рівня, кафедра програмного забезпечення систем, Дніпровський державний технічний університет
Anastasiia Tkach **Анастасія Ткач**	Student of the Department of Software Systems, Dniprovsky State Technical University https://orcid.org/0009-0002-7784-0684 e-mail: anastasiatkach920@gmail.com	Здобувач вищої освіти першого (бакалаврського) рівня, кафедра програмного забезпечення систем, Дніпровський державний технічний університет

https://doi.org/10.31891/csit-2025-2-13
UDK 004.9

BEDRATIUK Anna
Khmelnytskyi National University

METHOD FOR OBTAINING ROTATION-INVARIANT IMAGE REPRESENTATION BY REMOVING ORIENTATION FEATURES FROM AUTOENCODER LATENT SPACE

In many computer vision tasks, accurate object recognition is complicated by arbitrary object orientations. Ensuring rotation invariance is critical for improving classification accuracy and reducing errors related to the varying placement of objects. This issue is particularly important in real-world environments, where object orientation is rarely controlled.

The goal of this study is to develop a method that allows separating rotational features from the semantic essence of an object, while preserving high classification accuracy after removing orientation-related components. This approach enables the construction of models that remain effective under a wide range of input perspectives, thus improving robustness in practical applications.

The proposed method is based on using a convolutional variational autoencoder trained on a dataset of images subjected to various rotation angles. Linear regression is then used to identify those latent components that correlate most strongly with the rotation parameter. These components are removed, and the remaining features are used for classification. Additionally, image reconstruction is performed from the reduced latent vector to visually validate rotation invariance and evaluate the preservation of object shape.

Experiments on a synthetically rotated binarized digit dataset (modified MNIST) demonstrated that removing rotation-sensitive components led to a classification accuracy decrease of no more than 25–30% across latent space dimensions 3–10 (e.g., normalized accuracy dropped from 1.000 to 0.704 at d = 7). Reconstruction experiments showed that the semantic shape of digits was preserved, while specific orientation information was suppressed.

The scientific novelty of this work lies in introducing a simple and reproducible method for removing orientation-related features from the latent space of an autoencoder without modifying the model architecture or introducing specialized regularizers. The practical significance of the method is in reducing the influence of arbitrary object orientation on recognition accuracy, thereby increasing the universality and reliability of vision systems in uncontrolled settings. The proposed approach may be useful for building classifiers capable of handling images with varying or unknown orientations during data collection.

Keywords: variational autoencoder, feature disentanglement, rotation invariance, semantic representation, convolutional architecture, image classification, algorithms, machine learning

БЕДРАТЮК Ганна
Хмельницький національний університет

МЕТОД ОТРИМАННЯ ОБЕРТАЛЬНО-ІНВАРІАНТНОГО ПРЕДСТАВЛЕННЯ ЗОБРАЖЕНЬ ШЛЯХОМ ВИЛУЧЕННЯ ОЗНАК ОРІЄНТАЦІЇ З ЛАТЕНТНОГО ПРОСТОРУ АВТОКОДУВАЛЬНИКА

У багатьох задачах комп'ютерного зору ефективне розпізнавання об'єктів ускладнюється довільною орієнтацією об'єктів сцени. Забезпечення інваріантності до орієнтації є критичним для підвищення точності класифікації та зменшення помилок, пов'язаних із різним розташуванням об'єктів. Це особливо важливо в умовах реального середовища, де орієнтація об'єктів рідко є контрольованою.

Метою дослідження є розроблення методу, що дає змогу відокремити ознаки повороту від семантичної сутності об’єкта та зберегти здатність до високоточної класифікації після вилучення ознак, відповідальних за орієнтацію. Такий підхід сприяє побудові моделей, які залишаються ефективними навіть за різноманітних ракурсів вхідних даних, що підвищує їхню стійкість у практичних застосуваннях.

Запропонований метод базується на використанні згорткового варіаційного автокодера, який спочатку навчається на наборі зображень із різними кутами повороту. Після цього за допомогою лінійної регресії виявляються ті компоненти латентного простору, що найбільше корелюють із параметром повороту. Ці компоненти вилучаються, а решта ознак використовується для класифікації. Додатково відбувається відновлення зображень без вилучених компонент, що дає змогу візуально перевірити інваріантність до повороту та оцінити, наскільки ефективно зберігається розпізнавання форми об’єкта.

Експерименти на повернутому синтетичному бінаризованому наборі даних цифр (модифікований MNIST) показали, що видалення компонентів, чутливих до обертання, призводило до зниження точності класифікації не більше ніж на 25–30% для розмірностей латентного простору від 3 до 10 (наприклад, нормалізована точність зменшилася з 1.000 до 0.704 при d = 7). Експерименти з реконструкцією зображень показали, що семантична форма цифр зберігалася, тоді як інформація про конкретну орієнтацію пригнічувалася.

Наукова новизна дослідження полягає в тому, що вперше запропоновано простий та відтворюваний метод вилучення орієнтаційних ознак із латентного простору автокодера без потреби у модифікації архітектури моделі або застосування додаткових регуляризаторів. Практичне значення роботи полягає у зменшенні впливу довільної орієнтації об’єкта на точність розпізнавання, що дозволяє підвищити універсальність і надійність систем комп’ютерного зору в умовах неконтрольованого ракурсу. Отримані результати можуть бути використані для побудови класифікаторів, здатних ефективно працювати із зображеннями, у яких орієнтація об’єкта змінюється або не є фіксованою під час збирання даних.

Ключові слова: варіаційний автокодер, відокремлення ознак, інваріантність до повороту, семантичне подання, згорткова архітектура, класифікація зображень, машинне навчання

Introduction

In computer vision tasks, the accuracy of object classification heavily depends on the model's ability to account for geometric transformations, particularly arbitrary image rotations. In many practical applications — such as automatic recognition of biological structures, detection of material surface defects, or symbol recognition in digital documents — the position of the object in the image is uncontrollable. This creates a need for systems capable of recognizing objects independently of their orientation, i.e., possessing the property of rotation invariance.

Existing methods aimed at achieving such invariance often involve modifications to convolutional neural network architectures or the addition of special components to the loss function. However, these approaches tend to be complex to implement, computationally intensive, or lack interpretability. Recent attempts have been made to develop neural representations that explicitly separate object shape features from orientation information, but most of these solutions remain insufficiently transparent or difficult to reproduce. There is thus a need for a simple and interpretable approach that allows for the separation of rotation features without degrading classification quality.

The object of this study is the process of forming latent representations of images in neural networks used for classification tasks.

The subject of this study is the structure of the latent space of a convolutional variational autoencoder and its relationship to geometric transformations of input images, particularly rotations.

The aim of the work is to develop a method that enables the identification of latent space components responsible for object rotation and, based on the remaining components, to form an invariant semantic representation suitable for classification regardless of orientation.

To achieve this goal, the following tasks must be accomplished: – train a convolutional variational autoencoder on a dataset of images with varying rotation angles; – use linear regression to identify latent space components associated with rotation; – perform classification of images after removing these components; – reconstruct images using only non-rotation features and assess their quality; – investigate how well the removed components correspond to the rotation information.

The proposed approach addresses the existing gap between complex architectural solutions and the lack of controllability over the latent space. It allows for the construction of interpretable and practically usable object representations in tasks where geometric invariance is a crucial factor for recognition accuracy.

Problem statement

The task under consideration is to construct a latent representation of images that is invariant to the action of the rotation group $SO(2)$ in the image space. Let $X \subset \mathbb{R}^{H\times W}$ denote the set of input images (e.g., grayscale digit images of size 28×28 pixels) which can be arbitrarily rotated. Each image $x \in X$ is obtained as the result of the action of a certain rotation $g \in SO(2)$ on a "canonical" image $\tilde{x}$:

$$x = g \cdot \tilde{x}, \quad g \in SO(2).$$

Input variables:

- $x \in X$ — image with an unknown orientation;
- $\theta \in [-\pi, \pi)$ — (unobserved) rotation angle applied to the image;
- $y \in \{1, \dots, C\}$ — class label for the classification task.

Output variables:

- $z = f(x) \in \mathbb{R}^d$ — latent representation obtained via a function f implemented by a neural network (autoencoder);
- $z_{\text{sem}} \in \mathbb{R}^{d-k}$ — semantic part of the vector z with rotation-related components removed;
- $\hat{y} = h(z_{\text{sem}})$ — predicted class using only the semantic representation;
- $\hat{x} = \text{dec}(z_{\text{sem}})$ — reconstructed image recovered without rotation-related information.

Quality criteria:

- Minimization of the loss function $L = L_{\text{recon}} + L_{\text{KL}}$, characteristic for a variational autoencoder;
- Maximization of classification accuracy: $\mathbb{P}(\hat{y} = y)$;
- Interpretability of the influence of the components of the vector z on θ, assessed through the coefficients of a linear regression $\theta \sim z$;
- The quality of disentanglement is evaluated through the reconstruction of the image $\hat{x}$ from the invariant part z_{sem}.

Constraints:

- θ is not directly observed — its influence must be assessed indirectly;
- Removal of rotation-related components should minimally affect semantic content but significantly reduce dependence on orientation;
- The construction of z_{sem} should satisfy: $z_{\text{sem}}(g \cdot x) \approx z_{\text{sem}}(x)$ for all $g \in SO(2)$.

Thus, the goal is to construct a transformation function $f: X \to \mathbb{R}^d$ and a procedure for nullifying k components of the latent vector z such that the invariant part z_{sem} provides high classification and reconstruction performance independently of the input image rotation

Review of the literature

Ensuring invariance to geometric transformations, particularly rotations, constitutes one of the major challenges in contemporary deep learning. Convolutional neural networks (CNNs) exhibit local invariance to translations; however, they do not inherently guarantee invariance under the action of the SO(2) group without additional architectural modifications or specialized training procedures [1]. In response, several architectures have been proposed that are explicitly designed to achieve equivariance or invariance with respect to group actions. Notably, group-equivariant convolutional networks (G-CNNs) were introduced in [2], and subsequent works [3,4,5] further advanced this approach towards networks equivariant to continuous Lie groups.

Geometric deep learning, as a general paradigm, systematically investigates architectures grounded in symmetries and group actions [6]. A formal framework within this paradigm involves the use of equivariant convolutions as morphisms in the category of group representations [7,8]. Nevertheless, such architectures tend to be complex, challenging to scale, and often difficult to interpret.

Concurrently, a parallel research direction has focused on the development of latent representations that explicitly disentangle factors of variation, such as class, position, rotation, and scale. Beginning with [9], where β-VAE was proposed as a method for disentangling features, numerous VAE variants have been introduced to enable feature disentanglement at the latent level [10,11]. An illustrative example is Spatial-VAE [12], which models image content and spatial arrangement separately.

Recent literature has increasingly emphasized the integration of geometric symmetries into deep generative models. For instance, TARGET-VAE [13] incorporates group equivariance directly into the latent space. Related approaches include methods based on implicit neural representations (INRs), which combine hypernetworks with latent space regularization [14,15,16].

Despite considerable progress, significant limitations remain within existing approaches. Firstly, most methods for feature disentanglement are not explicitly tied to the mathematical structure of geometric symmetries, such as the SO(2) group. Secondly, even when invariance is achieved, it is often implicit, opaque, or obtained through complex architectural modifications. Thirdly, the relationship between classification accuracy degradation and the loss of geometric components in the latent space is rarely analyzed quantitatively.

The present work situates itself at the intersection of research on group action invariance and latent feature selection. In contrast to models such as β-VAE, where factor disentanglement is achieved implicitly via global modifications of the loss function, our approach explicitly and constructively enforces rotation invariance. This is accomplished by evaluating the correlation between latent components and the rotation parameter, followed by the removal of features most strongly associated with rotation. We propose a simple, transparent, and easily reproducible method for constructing rotation-invariant semantic representations based on a convolutional variational autoencoder, without modifying the architecture or introducing complex regularizers. This approach not only enhances interpretability but also enables a quantitative evaluation of the contribution of geometric features to overall classification performance. The method is applicable both to the theoretical analysis of latent space invariance and to the practical design of classifiers robust to input image orientation changes.

Proposed technique

In this study, a convolutional variational autoencoder (Conv-VAE) is employed, specifically designed for processing images with local structure. By local structure, we refer to the presence of spatial dependencies among neighboring pixels, forming characteristic patterns (such as edges, contours, or fragments of objects) that can be effectively extracted using convolutional filters.

The autoencoder consists of two components—the encoder and the decoder. The encoder receives the input image and, through a sequence of convolutional layers and nonlinear activations, transforms it into a feature vector, which is then fed into two separate fully connected layers. These layers produce the parameters of a multivariate latent normal distribution: a mean vector $\mu \in \mathbb{R}^d$ and a log-variance vector $\log\sigma^2 \in \mathbb{R}^d$, where d denotes the dimensionality of the latent space.

Based on these parameters, the model performs stochastic sampling using the so-called reparameterization trick. The latent vector $z \in \mathbb{R}^d$ is computed as:

$$z = \mu + \sigma \odot \varepsilon,$$

where $\sigma \in \mathbb{R}^d$ is the standard deviation vector reconstructed from $\log\sigma^2$, and $\varepsilon \in \mathbb{R}^d$ is a vector of random variables independently sampled from a standard normal distribution: $\varepsilon \sim \mathcal{N}(0, \mathbf{I})$. The operator $\odot$ denotes element-wise multiplication. This reparameterization separates the stochastic and deterministic parts of the sampling process, enabling optimization of the parameters μ and $\log\sigma^2$ via gradient backpropagation.

This representation enables stochastic encoding while maintaining differentiability, which is crucial for training using gradient-based methods.

The decoder performs the inverse transformation from the latent space back to the image space. It accepts the vector z and, through a sequence of transposed convolutional (or fully connected) layers, reconstructs an approximation $\hat{x}$ of the original image x. The autoencoder is trained by minimizing a loss function composed of two terms: the reconstruction error and the Kullback–Leibler divergence. The total loss function is given by:

$$\mathcal{L}(x, \hat{x}, \mu, \log\sigma^2) = \| x - \hat{x} \|^2 + D_{\mathrm{KL}}(\mathcal{N}(\mu, \sigma^2) \parallel \mathcal{N}(0, I)),$$

where the first term is the Euclidean norm of the difference between the input image x and its reconstruction $\hat{x}$, representing the reconstruction error. The second term is the Kullback–Leibler divergence between the approximate latent distribution $q(z|x) = \mathcal{N}(\mu, \sigma^2)$ and the prior distribution $p(z) = \mathcal{N}(0, I)$. In the notation $D_{\mathrm{KL}}(P \parallel Q)$, the symbol $\parallel$ denotes "relative to," indicating the direction of comparison: how much P diverges from Q, not the other way around. This regularization term encourages the latent variable distribution to remain close to the standard normal distribution, ensuring the consistency of the latent space structure.

Thus, the latent space is formed as a stochastic mapping of the input image into a multidimensional Euclidean space with a predefined dimensionality. During training, the network organizes the components of z such that individual dimensions correspond to the most significant factors of variation in the input data. In our case, we assume that one such factor may be the rotation angle of the object in the image, enabling further analysis of the model's invariance to the action of the group $SO(2)$.

For model training, we used the classic MNIST dataset of handwritten digits, containing grayscale images of size 28×28 pixels. To simplify the interpretation of results and to focus on geometric aspects of the representations, all images were binarized using a thresholding operation with a fixed threshold value $t = 0.5$. Thus, each pixel in the image takes a value of either 0 or 1, allowing us to treat the objects as pure geometric shapes without intensity variations.

To model the influence of geometric transformations, each base image x_0 was randomly rotated by an angle θ uniformly sampled from the interval $[-\pi, \pi)$. Formally, the transformed image x_θ is defined as the result of the action of a group element $g_\theta \in SO(2)$ on x_0, i.e.,

$$x_\theta = g_\theta \cdot x_0, \quad g_\theta \in SO(2),$$

where the action of g_θ is implemented as a rotation of the image around its center. This procedure injects the geometric factor of variation—the rotation angle—into the input data.

The use of the group $SO(2)$ is natural from the viewpoint of planar object symmetries, as it describes all possible object orientations without altering their shape. Thus, the constructed dataset enables the study of latent space invariance to the action of this group. In subsequent sections, we investigate the extent to which components of the latent vector z are sensitive to variations in θ, and whether it is possible to disentangle the influence of rotation from other semantic characteristics of the images.

After training the variational autoencoder model, each rotated image x_θ is associated with a corresponding latent vector $z \in \mathbb{R}^d$. Since the rotation angle θ is known for each image, it is possible to empirically evaluate the dependency of θ on the latent space components. To this end, an auxiliary linear regression task is considered, where θ is approximated by a linear combination of the components of z:

$$\theta = \beta_0 + \sum_{j=1}^{d} \beta_j z_j + \varepsilon,$$

where β_j are the regression coefficients and ε is the random error term. The goal of this regression is not to predict θ but to quantitatively identify which latent components are most sensitive to variations in orientation.

Based on the obtained coefficients β_j, their absolute values are computed, and the components z_j are ranked according to their influence on the rotation angle. Let $\mathcal{J}_\theta \subset \{1, \dots, d\}$ denote the subset of indices corresponding to the components with the largest absolute coefficients:

$$\mathcal{J}_\theta = \text{Top-}k(|\beta_1|, |\beta_2|, \dots, |\beta_d|),$$

where k is a predefined number of components considered rotation-sensitive. In typical experiments, values of $k = 2$ or 3 are used, depending on the total dimensionality of the latent space.

Following the identification of such components, a procedure is applied to modify the latent vector z by removing rotation-related information. This is achieved by zeroing out all components with indices in $\mathcal{J}_\theta$, while leaving the remaining components unchanged. Thus, the invariant part of the vector is formed as:

$$z_{\text{sem}} = \begin{cases} 0, & \text{if } j \in \mathcal{J}_\theta, \\ z_j, & \text{if } j \notin \mathcal{J}_\theta, \end{cases} \quad \text{for } j = 1, \dots, d.$$

The resulting vector z_{sem} is considered a semantic representation of the image, cleansed of rotation-related components. In the following sections, the effectiveness of this modification in preserving object semantics while mitigating the effect of orientation will be investigated.

Upon identifying the subset of latent components $\mathcal{J}_\theta$ most sensitive to image rotation, it becomes possible to construct a partial representation of the object that excludes information about its orientation. This representation should characterize only the semantic essence of the image—such as its class, shape, and stylistic features—and be invariant under the action of the group $SO(2)$.

Formally, the invariant vector z_{sem} is constructed by modifying the full latent vector z: all components with indices $j \in \mathcal{J}_\theta$ are zeroed out, while the others are left unchanged. Thus, a subspace of the latent space is defined in which information about rotation is either eliminated or minimized.

The requirement for invariance under the action of the rotation group $SO(2)$ is formulated as the approximate identity between vectors obtained from different orientations of the same object. Let x be an arbitrary image, and $g \in SO(2)$ be an arbitrary rotation, then we expect:

$$z_{\text{sem}}(g \cdot x) \approx z_{\text{sem}}(x), \quad \forall g \in SO(2),$$

where the action $g \cdot x$ denotes the rotation of the image x by the corresponding angle. This property implies that regardless of the object's orientation in the image, its invariant latent representation remains a stable descriptor of its shape and content.

This construction of z_{sem} enables the separation of semantic information from geometric factors, making it suitable for tasks such as classification, reconstruction, or comparison of objects independently of their orientation. Subsequently, we will evaluate the effectiveness of the invariant representation as an alternative to the full latent description.

For the experimental evaluation, a subset of 10,000 training images was used, generated by applying random rotations to the original MNIST dataset. All images were binarized and resized to a fixed dimension of 28×28 pixels. The dimensionality of the latent space, denoted by d, was predefined depending on the specific experiment, typically ranging from 5 to 10.

The experimental analysis involved three key procedures. First, object classification was performed using both the full latent vector z and the invariant representation z_{sem}, from which rotation-related components had been removed. This allowed for assessing how much information relevant to class recognition is preserved after the removal of geometric features.

Second, image reconstruction was performed based on both the full latent representation z and the invariant representation z_{sem}. This enabled visual comparison of how well the reconstructed images preserved the object's shape while mitigating or removing orientation information.

Third, an analysis of the impact of component removal on classification accuracy was conducted. This involved comparing classification results before and after removing the k most rotation-sensitive components. The value of k was determined experimentally, depending on the distribution of regression coefficients in the $\theta \sim z$ model.

The criteria for selecting components were based on the significance of the regression coefficients. Specifically, the components with the largest absolute contributions to the variation in the rotation angle were selected. All computations were performed after training the Conv-VAE with a fixed architecture, without further fine-tuning of the network weights.

Detailed quantitative evaluations and interpretations of these procedures will be presented in the following section.

Experiments

The experimental part of this study is based on a step-by-step analysis of the latent space of a convolutional variational autoencoder (Conv-VAE) to identify and eliminate components responsible for the object's rotation. The general scheme of the experiments involves several key steps.

In the first stage, the Conv-VAE model is trained on a modified version of the classic MNIST dataset, where random image rotations within the angle range $\theta \in [-\pi, \pi)$ have been applied. As a result of training, each image is associated with a latent vector $z \in \mathbb{R}^d$, representing its internal representation in the model's latent space.

The next step involves constructing a linear regression model that approximates the rotation angle θ as a linear function of the components of z. This allows for a quantitative assessment of the influence of each component z_j on the geometric property of orientation. Components with the largest regression coefficients are interpreted as those containing information about rotation. Subsequently, a modified vector z_{sem} is constructed, in which the identified rotation-sensitive components are zeroed out. This vector is considered an invariant representation of the image, preserving its semantic essence while eliminating orientation information. In subsequent experiments, classification accuracy is compared between the full latent representation z and the cleaned representation z_{sem}. Additionally, the quality of image reconstruction based on both types of vectors is investigated, allowing for an evaluation of the impact of component removal on the visual interpretation of the image. The proposed scheme is universal and can be replicated using any dataset where geometric factors of variation are explicitly or implicitly present.

The experiments were conducted using the publicly available MNIST dataset, containing 60,000 grayscale images of handwritten digits with a resolution of 28×28 pixels. Since the study aims to investigate invariance to the action of the rotation group $SO(2)$, the base dataset was modified by applying a random rotation to each image.

Specifically, for each image x_0 from the original dataset, a new image x_θ was generated by rotating it by a random angle θ uniformly sampled from the interval $[-\pi, \pi)$. Formally, the transformed image is written as $x_\theta = g_\theta \cdot x_0$, where $g_\theta \in SO(2)$ is the operator corresponding to a rotation by θ around the image center. The value of θ

was stored in the metadata for each image, enabling its use as a regression variable for analyzing the latent space structure.

Following rotation, each image underwent a binarization procedure. A fixed threshold $t = 0.5$ was applied: pixels with intensities above the threshold were set to 1, and those below to 0. This approach removes intensity variation effects and focuses attention solely on geometric properties such as shape and orientation.

Thus, the prepared dataset preserves the key semantic information about the digit class while introducing an independent variable—the rotation angle—creating favorable conditions for analyzing the model's ability to separate geometric from semantic features in latent representations.

The models were trained using a convolutional variational autoencoder architecture adapted for binarized 28×28 pixel images. The encoder consisted of two convolutional layers with ReLU activation, followed by a flattening operation and two separate fully connected layers generating the mean vector $\mu \in \mathbb{R}^d$ and the log-variance vector $\log\sigma^2 \in \mathbb{R}^d$ for the latent normal distribution. The decoder implemented the reverse mapping using one or two fully connected layers followed by nonlinearities, ending with a layer that produced the final image using a sigmoid activation function.

The latent space dimensionality d varied within the range $5 \leq d \leq 10$, depending on the specific experiment. For each value of d, the model was trained separately. Training was performed on 10,000 rotated images for 5 epochs using mini-batches of size 64. The Adam optimizer was used with a fixed learning rate of 10^{-3} and default hyperparameters.

The loss function followed the standard formulation for variational autoencoders, consisting of two terms: the reconstruction error and the Kullback–Leibler divergence. The reconstruction error was calculated as the sum of binary cross-entropy losses between the original and reconstructed images, an appropriate choice for binary pixel values. The regularization term encouraged the posterior distribution of latent variables to approximate a standard normal distribution.

All experiments were conducted in Python using the PyTorch framework. Training was performed on an NVIDIA Tesla T4 GPU in the Google Colab cloud environment. To ensure reproducibility, the random seed was fixed across all experiments. The model architecture, training hyperparameters, and data structure were kept constant, except for the latent space dimensionality d.

To evaluate the effectiveness of the proposed approach to invariant latent representation construction, several experimental scenarios were implemented, each corresponding to a specific aspect of testing the hypothesis of disentangling rotation information from the semantic content of the image.

In the first scenario, classification was performed using the full latent vector z obtained after encoding. A linear classification model was trained on a subset of the dataset with known class labels. This served as a baseline reflecting the maximum achievable classification accuracy with complete information.

The second scenario repeated the classification procedure, but using the modified vector z_{sem}, where the rotation-related components had been zeroed out according to the regression model. This experiment aimed to assess changes in classification accuracy when orientation information is removed from the latent representation.

The third experiment focused on a visual assessment of the effect of removing rotation components. Images were reconstructed from both the full vector z and the cleaned vector z_{sem}. This comparison allowed evaluation of how well the object's geometric shape was preserved and whether the orientation was altered or suppressed. The final scenario addressed the stability of the method under different rotation angles. Subsets of images with specific, uniformly distributed values of θ were selected. Within each subset, images were reconstructed and visually compared. This allowed verification of whether z_{sem} remains invariant under the action of $SO(2)$, regardless of the particular rotation angle.

All the above scenarios are complementary and cover both quantitative and qualitative aspects of analysis—classification accuracy, geometric integrity of reconstructions, and model behavior under orientation variations. The results of each scenario will be presented in the next section.

To ensure scientific reproducibility of the experiments, several procedures were followed to maintain stability and minimize random effects. All computations were performed with a fixed initial random seed, ensuring that results could be replicated upon re-execution.

Models were trained multiple times with the same hyperparameters but different random weight initializations, demonstrating the stability of the architecture against parameter fluctuations. Key metrics—classification accuracy, regression R^2 scores, and reconstruction error—were averaged over multiple runs to improve the reliability of the obtained estimates.

For visual analysis of model behavior at different rotation angles, controlled subsets of images with fixed θ values were formed. This avoided dependence on the random distribution of the full dataset and ensured uniform coverage of the $SO(2)$ action space. Furthermore, the stability of rotation-sensitive component detection was assessed by comparing linear regression coefficients $\theta \sim z$ across different training runs. Consistency in the dominant components provided additional confirmation of the structural informativeness of the latent space.

Thus, all stages of the experimental protocol were organized to ensure that the results could be confidently interpreted as robust, statistically valid, and independently verifiable by any qualified researcher.

Results

To assess the impact of removing rotation-sensitive components on the model's classification ability, a comparison of two scenarios was conducted:

In the first scenario, images were classified based on the full latent vector $\mathbf{z}$ obtained after encoding. Logistic regression was applied to each sample with its class label preserved, trained on a subset of the data. This scenario served as a baseline reflecting the maximum achievable classification accuracy under complete information.

The second scenario repeated the classification procedure but used the modified vector $\mathbf{z}_{\text{sem}}$, where the components associated with the rotation angle θ were zeroed out according to the regression model. The aim of this experiment was to identify changes in classification accuracy when orientation information is removed from the latent representation.

The results for different latent space dimensions are presented in Table 1. In addition to the actual classification accuracies for both scenarios, the relative classification accuracy loss (if the first scenario is taken as 100%) is shown. The last column indicates how much information is *not* captured by the most rotation-sensitive components (i.e., the complement to 100%).

Table 1

Comparison of classification accuracy in two scenarios (logistic regression)

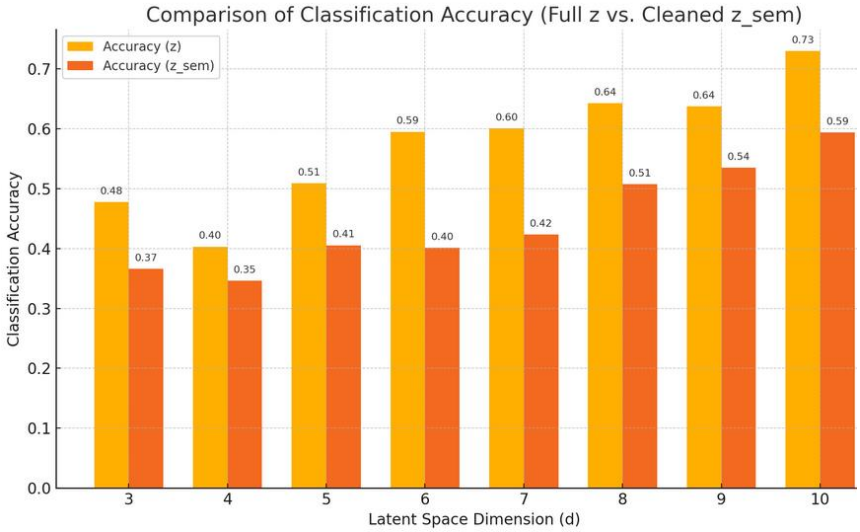
d	Accuracy z	Accuracy z_{sem}	Accuracy loss (%)	100% − sum of contributions (%)
3	0.4775	0.3659	23.37	49.38
4	0.4032	0.3465	14.06	22.09
5	0.5093	0.4055	20.38	39.26
6	0.5950	0.4016	32.50	19.06
7	0.6008	0.4233	29.54	37.12
8	0.6428	0.5072	21.12	26.83
9	0.6377	0.5350	16.13	26.78
10	0.7296	0.5941	18.60	23.61

The table analysis shows that removing only the latent components most contributing to the rotation regression indeed leads to a reduction in classification accuracy. This reduction reflects not only the loss of geometric information but also, partially, the loss of semantic features not completely orthogonal to orientation-sensitive components. The last column represents the fraction of information *not* contained in the most rotation-sensitive components, interpreted as an upper bound for the semantic information preserved in the vector $\mathbf{z}_{\text{sem}}$ after removing orientation features.

For example, if the sum of contributions of removed components is 70%, the remaining 30% of information could be used for classification independently of the object's orientation. This leftover is expected to correlate with the post-removal classification accuracy: the more information is preserved, the smaller the accuracy drop. Such a metric helps not only to quantitatively evaluate the "cleanliness" of the representation but also to explain the empirically observed degradation in classification performance.

Thus, the proposed approach allows for a quantitative assessment of the role of orientation-related features in the latent representation and provides an empirical basis for the construction of invariant classifiers.

For better visualization of the effect of removing rotation-sensitive components, a plot (Fig.1)



Fig, 1 Normalized classification accuracy for the full and cleaned latent representations

was created showing the classification accuracy for the two scenarios: with the full latent vector $\mathbf{z}$ and with the cleaned representation $\mathbf{z}_{\text{sem}}$. The plot also presents the relative loss of accuracy, allowing a quantitative evaluation of the role of orientation features. It can be seen that although the accuracy decreases after vector cleaning, the preserved portion of performance remains high, indicating effective preservation of semantic content in $\mathbf{z}_{\text{sem}}$.

To assess the influence of individual latent components on the object's orientation, a linear regression model approximating the rotation angle θ from the latent vector $z \in \mathbb{R}^d$ was constructed:

$$\theta = \beta_0 + \sum_{j=1}^{d} \beta_j z_j + \varepsilon,$$

where β_j are the weights for the j-th component and ε is the random error. From this model, the coefficients β_j and the coefficient of determination R^2 (characterizing the regression's precision) were calculated.

For latent space dimensionality $d = 7$, the regression model yielded $R^2 = 0.5402$, indicating a substantial but not complete dependence between rotation and latent components. The largest contribution was found for component z_5 with $|\beta_5| = 14.23$.

To formalize the contribution of each component to the variability of the rotation angle, normalized squared coefficients were computed:

$$\rho_j = \frac{\beta_j^2}{\sum_{k=1}^{d} \beta_k^2},$$

representing the fraction of explained variance per component. The corresponding ρ_j values are provided in Table 2.

Table 2

Latent component contributions to rotation regression for $d = 7$

Component z_j	Contribution ρ_j (%)
z_0	9.32
z_1	4.43
z_2	21.77
z_3	5.26
z_4	1.91
z_5	40.56
z_6	16.76

As shown in the table, the main information about rotation is concentrated in three components — z_2, z_5, and z_6 — whose combined contribution exceeds 80%. This suggests that removing these components should effectively eliminate orientation information while minimizing the loss of semantic content. This approach will be further tested in subsequent subsections, particularly during image reconstructions.

To evaluate the influence of rotation-sensitive components on image structure, reconstructions were performed in two ways: based on the full latent representation z and based on the cleaned representation z_{sem}, from which components z_2, z_5, and z_6 — most correlated with the rotation angle — were removed.

Figure 2 shows examples of such reconstructions. In each row, the left column shows the input rotated image x_θ, the middle column shows the reconstruction from the full vector z, and the right column shows the reconstruction from z_{sem}. All reconstructions were performed using the same decoder without retraining.

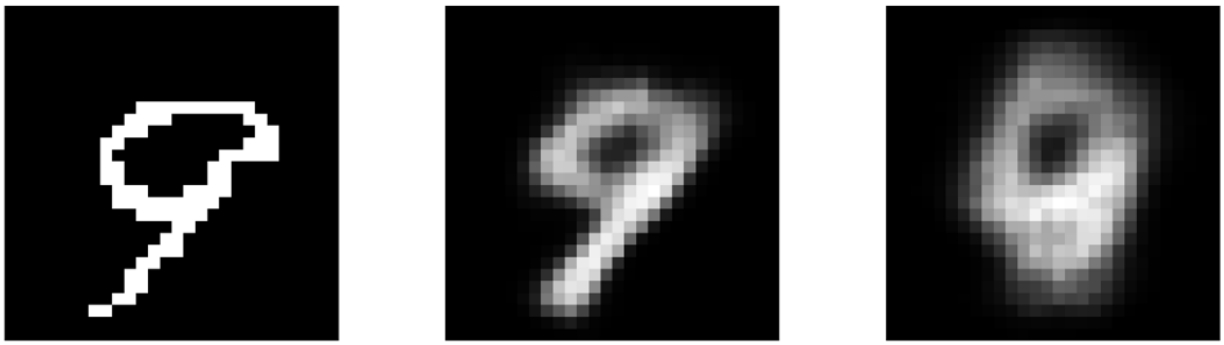


Fig. 2 Examples of reconstructions: left — input rotated image, center — reconstruction from z, right — reconstruction from z_{sem}

The graphical results indicate that reconstructions based on the full latent vector $\mathbf{z}$ recover both the general shape and the orientation of the object. In contrast, reconstructions from the cleaned vector $\mathbf{z}_{\text{sem}}$, with rotation-related components removed, show a loss of geometric orientation information: the object remains recognizable but

appears less oriented or more generalized in shape. Nevertheless, the distinctive digit shape is preserved in most cases, confirming that semantic structure is retained after removing orientation features.

It should be emphasized that the cleaned representation does not attempt to explicitly compensate for the rotation or realign the object along any fixed axis. Instead, the removal of rotation components results in the loss of specific orientation information, which cannot be recovered by the decoder without access to the removed variables. This illustrates the effect of achieving rotation invariance at the reconstruction level.

These results visually confirm that the removed components indeed encode information about orientation, while the remaining latent space primarily encodes the object's shape and class. More examples will be presented in the next subsection, where reconstruction under fixed rotation angles is analyzed.

At the same time, the characteristic shape of the digit is preserved in most cases, indicating that the semantic structure of the representation remains intact after the removal of orientation features. It should be emphasized that the cleaned representation does not explicitly attempt to compensate for the rotation or to align the image along any fixed axis. Instead, the removal of rotation-sensitive components leads to a loss of specific orientation information, which cannot be recovered by the decoder without access to the removed variables. This illustrates the effect of achieving rotation invariance at the level of reconstruction.

The observed degradation in reconstruction quality after the removal of rotation-sensitive components can be explained by the fact that these components, in addition to containing orientation information, also partially encode other features important for accurate image reproduction. Consequently, their removal results not only in the loss of orientation information but also in a partial reduction of the overall expressiveness of the latent representation, which affects reconstruction quality.

Consider a hypothetical situation where a single latent component contains all the information about the image's rotation, being fully responsible for the object's orientation. In such a case, removing this component would eliminate the orientation information without affecting other aspects of the image, such as its shape, structure, or semantic essence. As a result, the reconstruction quality would remain high, and the object would retain its recognizability — only without a specific orientation.

These results visually confirm that the removed components indeed encode information about orientation, while the remaining latent space is primarily responsible for capturing the object's shape and class. The next subsection analyzes the stability of these results across different latent space dimensionalities.

To test the generalizability and robustness of the proposed approach, a series of experiments was conducted for different latent space dimensions $d \in \{3,4,5,6,7,8,9,10\}$. For each value of d, a Conv-VAE model was trained from scratch, and all methodological steps were applied sequentially: regression $\theta \sim \mathbf{z}$, identification of rotation-sensitive components, formation of the cleaned representation $\mathbf{z}_{\text{sem}}$, classification, and image reconstruction.

The classification results are presented in Table 3 in the form of normalized accuracy (relative to the full latent vector $\mathbf{z}$). As shown, the removal of rotation-sensitive components leads to some loss in accuracy in each case; however, the loss is never critical. For smaller dimensions d, the losses are larger, which can be explained by the smaller capacity of the space and the higher relative contribution of rotation information.

Table 3.

Normalized classification accuracy for different latent space dimensions d

d	Accuracy z (normalized)	Accuracy z_{sem} (normalized)
3	1.000	0.766
4	1.000	0.859
5	1.000	0.796
6	1.000	0.675
7	1.000	0.704
8	1.000	0.789
9	1.000	0.839
10	1.000	0.814

The values of the coefficient of determination R^2 for the regression of the rotation angle θ onto the full vector $\mathbf{z}$ remained stable within the range $[0.47,0.53]$ across all d. This confirms the consistency of the geometric signal within the latent representation. In all cases, the rotation-sensitive information was concentrated in 2–3 latent components with the highest regression coefficients. The proportion of preserved information after cleaning correlated well with the classification accuracy based on $\mathbf{z}_{\text{sem}}$.

Thus, the effects of removing orientation features are stable across different latent space dimensionalities and are not artifacts of the choice of d. This supports the generalizability of the invariant representation method and its applicability to a wider range of tasks.

Discussion

The obtained results confirm the main hypothesis of this study: within the latent space of a variational autoencoder, there exists a subspace responsible for the geometric orientation of an object, specifically its rotation angle. Identifying such rotation-sensitive components using linear regression and subsequently removing them

enables the construction of a latent representation that exhibits invariance properties with respect to the action of the group SO(2). Experiments demonstrated that this structure of the latent space consistently emerges across different latent dimensions d, with the geometric information concentrated in only 2–3 components, making the task of detection and removal interpretable.

The comparison between the full latent representation z and the invariant variant $\mathbf{z}_{sem}$ showed that even after the removal of several key components, classification accuracy decreased only partially. According to the data presented in the tables, the performance loss rarely exceeded 25–30%, and in some cases, remained within the bounds of statistical error. This indicates that the remaining components of the latent vector predominantly contain semantic information that is weakly dependent on the object's orientation. Visual reconstructions confirmed that objects lost specific geometric orientation features but retained their recognizable shape. Compared to approaches like TARGET-VAE or Spatial-VAE, the proposed method offers several advantages. It does not require modification of the network architecture, introduction of additional regularizers, or use of group convolutions as in works employing equivariance. Instead, the method relies on a simple empirical procedure of latent space analysis after training, making it compatible with any VAE variants, including β-VAE or INR-based models.

Despite its simplicity and effectiveness, the proposed approach has several limitations: (i) the rigid zeroing of rotation-sensitive components can distort the structure of the latent space and degrade the quality of generated or reconstructed images; (ii) the method does not guarantee full rotation invariance, as residual orientation-related information may remain in other components; (iii) the current approach is specific to rotation invariance and does not directly address other geometric transformations such as scaling, translation, or perspective changes; generalization would require extension to larger symmetry groups (e.g., SE(2), SIM(2)); (iv) removing components without considering their interactions with other latent variables may lead to unintended loss of useful information beyond rotation features.

Nevertheless, the method demonstrates high efficiency in tasks where rotation invariance is a desirable property. It can be applied as a preprocessing step in classification, clustering, or latent space analysis pipelines. Moreover, the proposed approach enables better interpretability of the internal structure of VAE models and serves as a foundation for further research in the direction of automatic extraction and segmentation of factors of variation.

Conclusions

In this study, a method for constructing an invariant latent representation of images, insensitive to rotations, was proposed. The approach is based on an empirical analysis of the latent space of a convolutional variational autoencoder (Conv-VAE) and involves building a linear regression of the rotation angle θ on the components of the latent vector z, followed by the removal of the most rotation-sensitive features. The method does not require any architectural modifications or the use of special regularizers, making it universal and suitable for integration with various types of deep learning models.

Scientific novelty — For the first time, it has been demonstrated that geometric information about an object's orientation can be successfully localized in a few latent components, identified through a simple regression model. An effective procedure for removing such components has been proposed, allowing the construction of representations that are approximately invariant to the action of the SO(2) group without additional architectural complexity.

Achieved results — Experiments on the modified (rotated) MNIST dataset showed that classification accuracy using the cleaned representation $\mathbf{z}_{sem}$ decreased by no more than 25–30% compared to the full latent representation, across latent space dimensions $d \in [3, 10]$. For example, at d = 7, normalized accuracy decreased from 1.000 to 0.704. The object's shape was preserved after removing rotation-sensitive components, while orientation information was visually neutralized. The method consistently localized geometric factors in 2–3 components and demonstrated stability across varying latent space dimensions.

Practical significance, limitations, and future prospects — The method can be applied in tasks where object orientation is random, variable, or hinders precise analysis, such as in biomedical imaging, quality control, visual inspection, and natural scenes. However, several limitations should be noted: (i) some residual rotation information may remain in the cleaned latent representation; (ii) the rigid zeroing of components can reduce reconstruction quality and generative capability; (iii) extension to more complex transformations (e.g., scale, translation) requires further development. Future work could focus on generalizing the approach to other symmetry groups (e.g., SE(2)), developing softer mechanisms for information removal (e.g., orthogonal projections), and applying the method under unsupervised learning conditions or in combination with implicit neural representations (INRs).

References

1. Sitzmann V. Implicit neural representations with periodic activation functions / V. Sitzmann, J. Martel, A. Bergman, D. Lindell, G. Wetzstein // Advances in neural information processing systems. – 2020. – Vol. 33. – P. 7462-7473. DOI: 10.48550/arXiv.2006.09661

2. Wiesner D. Implicit neural representations for generative modeling of living cell shapes / D. Wiesner, J. Suk, S. Dummer, D. Svoboda, J. M. Wolterink // International Conference on Medical Image Computing and Computer-Assisted Intervention : proceedings. – Berlin : Springer, 2022. – P. 58-67. DOI: 10.1007/978-3-031-16440-8_6

3. Tancik M. Fourier features let networks learn high frequency functions in low dimensional domains / M. Tancik, P. Srinivasan, B. Mildenhall, S. Fridovich-Keil, N. Raghavan, U. Singhal, R. Ng // Advances in neural information processing systems. – 2020. – Vol. 33. – P. 7537-7547. DOI: 10.48550/arXiv.2006.10739
4. Cohen T. Group equivariant convolutional networks / T. Cohen, M. Welling // International conference on machine learning : proceedings. – PMLR, 2016. – P. 2990-2999. DOI: 10.48550/arXiv.1602.07576
5. Weiler M. General e (2)-equivariant steerable CNNs / M. Weiler, G. Cesa // Advances in neural information processing systems. – 2019. – Vol. 32. DOI: 10.48550/arXiv.1911.08251
6. Weiler M. Equivariant and Coordinate Independent Convolutional Networks: A Gauge Field Theory of Neural Networks / M. Weiler. – University of Amsterdam, 2023. – (PhD Thesis). DOI: 10.1142/14143
7. Bronstein M. M. Geometric deep learning: Grids, groups, graphs, geodesics, and gauges / M. M. Bronstein, J. Bruna, T. Cohen, P. Veličković. DOI: 10.48550/arXiv.2104.13478
8. Finzi M. Generalizing convolutional neural networks for equivariance to Lie groups on arbitrary continuous data / M. Finzi, S. Stanton, P. Izmailov, A. G. Wilson // International Conference on Machine Learning : proceedings. – PMLR, 2020. – P. 3165-3176. DOI: 10.48550/arXiv.2002.12880
9. Bekkers E. J. B-spline CNNs on lie groups / E. J. Bekkers. DOI: 10.48550/arXiv.1909.12057
10. Higgins I. beta-VAE: Learning basic visual concepts with a constrained variational framework / I. Higgins, L. Matthey, A. Pal, C. Burgess, X. Glorot, M. Botvinick, A. Lerchner // International conference on learning representations : proceedings. – 2017. https://openreview.net/pdf?id=Sy2fzU9gl
11. Chen R. T. Isolating sources of disentanglement in variational autoencoders / R. T. Chen, X. Li, R. B. Grosse, D. K. Duvenaud // Advances in neural information processing systems. – 2018. – Vol. 31. DOI: 10.48550/arXiv.1802.04942
12. Locatello F. Challenging common assumptions in the unsupervised learning of disentangled representations / F. Locatello, S. Bauer, M. Lucic, G. Raetsch, S. Gelly, B. Schölkopf, O. Bachem // International conference on machine learning: Proceedings. – PMLR, 2019. – P. 4114-4124. https://proceedings.mlr.press/v97/locatello19a/locatello19a.pdf
13. Bepler T. Explicitly disentangling image content from translation and rotation with spatial-VAE / T. Bepler, E. Zhong, K. Kelley, E. Brignole, B. Berger // Advances in Neural Information Processing Systems. – 2019. – Vol. 32. https://proceedings.neurips.cc/paper_files/paper/2019
14. Kwon S. Rotation and translation invariant representation learning with implicit neural representations / S. Kwon, J. Y. Choi, E. K. Ryu // International Conference on Machine Learning : proceedings. – PMLR, 2023. – P. 18037-18056. DOI: 10.48550/arXiv.2304.13995
15. Liu R. An intriguing failing of convolutional neural networks and the coordconv solution / R. Liu, J. Lehman, P. Molino, F. Petroski Such, E. Frank, A. Sergeev, J. Yosinski // Advances in neural information processing systems. – 2018. – Vol. 31. DOI: 10.48550/arXiv.1807.03247
16. Achille A. Emergence of invariance and disentanglement in deep representations / A. Achille, S. Soatto // Journal of Machine Learning Research. – 2018. – Vol. 19(50). – P. 1-34. DOI: 10.1109/ITA.2018.8503149

Anna Bedratiuk **Ганна Бедратюк**	Senior Lecturer at the Department of Software Engineering, Khmelnytskyi National University, Khmelnytskyi, Ukraine https://orcid.org/0000-0003-0224-5549 e-mail: bedratyuk@ukr.net	Старший викладач кафедри інженерії програмного забезпечення, Хмельницький національний університет

https://doi.org/10.31891/csit-2025-2-14
UDC 004.49

RAMSKYI Ihor, DROZD Andriy, LYHUN Oleksii
Khmelnytskyi National University

SYSTEM FOR CYBERSECURITY EVALUATION OF CORPORATE NETWORKS

In the context of rapidly increasing cyber threats and the growing complexity of corporate IT infrastructure, ensuring a reliable and proactive approach to cybersecurity is becoming critically important for organizations of all sizes. Traditional cybersecurity assessment methods often fail to keep up with the dynamic nature of emerging threats – necessitating the development of more adaptive and intelligent evaluation systems. This article presents a comprehensive modular system for assessing the cybersecurity level of corporate networks – offering a holistic view of the security landscape by integrating both technical and organizational indicators.

The proposed system utilizes self-organizing analytical methods to dynamically process large volumes of data related to vulnerabilities, configuration states, and network behavior patterns. Through intelligent algorithms and adaptive learning, the system is capable of autonomously detecting anomalies, evaluating potential attack vectors, and correlating threats with the network's weak points. Additionally, the inclusion of organizational factors – such as policy compliance, user behavior, and access structures – enables a more contextual and in-depth risk assessment.

A key advantage of the system is its ability to perform real-time monitoring and dynamic risk evaluation – empowering decision-makers to take informed actions in response to incidents. The system's architecture supports scalability and compatibility with existing security tools and network management platforms.

To validate its effectiveness, the system was implemented and tested in a simulated corporate environment reflecting modern structural and operational challenges. The experimental results confirmed its capability to identify vulnerabilities, prioritize responses, and enhance overall cyber resilience.

This research contributes to the advancement of next-generation cybersecurity assessment tools – ensuring the continuous improvement of corporate defense mechanisms in an ever-changing cyber landscape.

Keywords: Corporate networks, distributed systems, cybersecurity

РАМСЬКИЙ Ігор, ДРОЗД Андрій, ЛИГУН Олексій
Хмельницький національний університет

СИСТЕМА ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

У контексті стрімкого зростання кіберзагроз та зростаючої складності корпоративної IT-інфраструктури забезпечення надійного та проактивного підходу до кібербезпеки стає критично важливим для організацій будь-якого масштабу. Традиційні методи оцінювання кібербезпеки часто не встигають за динамікою змін у загрозах, що зумовлює необхідність розробки більш адаптивних та інтелектуальних систем оцінки. У цій статті представлено комплексну модульну систему для оцінки рівня кібербезпеки корпоративних мереж, яка забезпечує цілісне бачення безпекової ситуації шляхом інтеграції як технічних, так і організаційних показників.

Запропонована система використовує самоорганізуючі аналітичні методи для динамічної обробки великих обсягів даних про вразливості, конфігураційні стани та поведінкові особливості мережі. Завдяки інтелектуальним алгоритмам та адаптивному навчанню система здатна автономно виявляти аномалії, оцінювати потенційні вектори атак і співвідносити загрози з вразливими місцями системи. Додатково, врахування організаційних факторів – таких як відповідність політикам, поведінка користувачів та структура доступу – забезпечує більш контекстуальну та глибоку оцінку ризиків.

Однією з ключових переваг системи є можливість здійснення моніторингу в реальному часі та динамічної оцінки ризиків, що дозволяє керівникам приймати обґрунтовані рішення для своєчасного реагування на інциденти. Архітектура системи передбачає масштабованість і сумісність з існуючими засобами захисту та платформами управління мережею.

Для підтвердження ефективності система була реалізована та протестована у моделюваному корпоративному середовищі, що відображає сучасні структурні та операційні виклики. Результати експерименту підтвердили її здатність виявляти вразливості, визначати пріоритети реагування та зміцнювати загальну кіберстійкість.

Це дослідження робить внесок у розвиток інструментів оцінювання кібербезпеки нового забезпечуючи постійне вдосконалення корпоративних механізмів захисту в умовах мінливого кіберсередовища.

Ключові слова: корпоративні мережі, розподілені системи, кібербезпека.

Introduction

In today's digitally interconnected world, corporate networks have become critical infrastructures that support core business operations, data exchange, and communication processes. As organizations increasingly rely on complex information systems, the potential attack surface expands, exposing networks to a broad range of cyber threats. These threats – ranging from malware and ransomware to advanced persistent threats and insider attacks – continue to grow in sophistication, frequency, and impact. Consequently, ensuring the cybersecurity of corporate networks has evolved from a technical challenge into a strategic necessity for maintaining operational continuity, protecting sensitive data, and preserving stakeholder trust.

Traditional cybersecurity assessment methods often rely on periodic audits, rule-based monitoring, or reactive measures that are insufficient in addressing modern, dynamic threat landscapes. Static approaches fail to capture real-time changes in network topology, user behavior, or system configurations, limiting their effectiveness in identifying and mitigating emerging threats. Furthermore, many existing solutions focus primarily on technical

vulnerabilities while neglecting the organizational and procedural factors that also influence the overall security posture.

To address these limitations, there is a growing need for adaptive, comprehensive systems capable of continuously evaluating the cybersecurity state of corporate networks. Such systems should integrate both technical and organizational indicators, provide real-time insights, and support proactive risk management strategies.

This article presents a novel system for cybersecurity evaluation designed specifically for corporate networks. The system incorporates self-organizing analytical methods to interpret vulnerability data, configuration states, and behavioral patterns across the network. It enables real-time monitoring, dynamic risk assessment, and prioritization of mitigation efforts based on contextual analysis. The architecture is modular and scalable, allowing for seamless integration into diverse IT environments.

The following sections describe the system's design and implementation, followed by an evaluation of its performance within a simulated enterprise environment. The results demonstrate the system's ability to enhance situational awareness, support decision-making, and improve the overall cybersecurity resilience of corporate networks.

Related works

Assessing cybersecurity in corporate networks requires sophisticated methods for detecting and responding to various threats. Modern corporate networks function as distributed systems with partial centralization, where decision-making on malware detection is structured as a decentralized subsystem. The use of characteristic indicators and analytical models allows the system to evaluate the constituent states and determine the corresponding reactions. Among the existing approaches, there is one that combines several methods for detecting malware, treating system components as integral sensors [1][2].

Ensuring resilience to cyberattacks, particularly botnets, is a critical aspect of cybersecurity assessment. The reviewed literature provides an example of a self-adaptive system for reconfiguring corporate networks based on security scenarios obtained as a result of cluster analysis of network traffic features. Using a semi-supervised fuzzy c-means clustering approach, the system detects cyber threats and selects security strategies to mitigate botnet attacks, increasing network resilience [3]. Another three-tier botnet detection system model provides the ability to identify both known and unknown botnets by combining host-level Bayes classification with network-level extensions. This approach allows for efficient exchange of information in a distributed system and has demonstrated promising results in the accuracy of botnet detection [4].

Distributed denial-of-service (DDoS) attacks are another major cybersecurity issue, especially in software-defined networks (SDNs). To detect and mitigate these attacks, a machine learning-based framework has been developed that uses the Support Vector Classifier and the Gradient Boost Classifier (SVC-GBC). With 99.4% accuracy, this hybrid approach significantly improves SDN security by refining detection granularity and strengthening defense mechanisms [5]. In addition to intrusion detection, anomaly detection in distributed systems remains a challenge due to complex dependencies between system logs. A deep learning-based Time Logical Attention Network (TLAN) has been introduced to model both time series patterns and logical dependencies, improving anomaly detection performance while reducing false signals [6].

The reliability of cybersecurity assessments in distributed systems is further enhanced by failure detection mechanisms. These mechanisms monitor the activity of nodes to identify faults and increase the fault tolerance of the system. Systematic analysis of fault detectors in distributed environments highlights their role in ensuring the reliability of services by solving matching and failure problems [7]. Log-based anomaly detection (LAD) also plays an important role in cybersecurity assessment, using system logs to identify potential threats and service anomalies. The overall structure of LAD for distributed systems includes logging grouping and feature mining to improve detection efficiency, demonstrating its applicability in real-world distributed environments [8].

In addition, privacy issues in distributed computing require robust security systems. The study of privacy in distributed systems focuses on the risks associated with data evaluation and information tracking, emphasizing the relevance of zero-trust security models for the secure implementation of systems in cloud architectures [9]. As the complexity of distributed systems continues to grow, effective system audit mechanisms that combine advanced analytics and artificial intelligence are becoming important for vulnerability monitoring and improving security [10].

These advances together contribute to the creation of a comprehensive cybersecurity assessment system that ensures the resilience of corporate networks to evolving threats. Cybersecurity assessments in corporate networks should address issues related to reliability, anomaly detection, and compliance with security policies. The zero-trust security model emphasizes the need to validate on-premises servers on corporate intranets, however, existing certification methods remain unavailable to small organizations due to cost and complexity. This gap leads to dependence on self-signed certificates, increasing vulnerability to impersonation and unauthorized access, which ultimately violates the principles of zero trust [11]. To improve the detection of security threats in large-scale distributed systems, a federated approach based on learning has been proposed, integrating multimodal large language models. This system handles a variety of data sources, achieving 96.4% accuracy while maintaining data confidentiality and computational efficiency, demonstrating significant improvements over traditional detection methods [12].

Anomalies in distributed systems pose significant risks due to time delays and deterioration in data quality. A deep learning-based real-time data quality assessment system has been implemented, which uses adaptive neural networks and parallel processing to provide scalable, low-latency anomaly detection. Evaluations on large-scale datasets confirm the system's effectiveness in maintaining high detection accuracy when processing more than 1.2 million events per second [13]. In cloud computing environments, optimizing resource allocation is critical to maintaining efficiency. Machine learning-based approaches, combining deep learning and genetic algorithms, have been developed to improve resource planning, addressing issues such as load imbalances and low utilization [14].

Further advances in distributed computing focus on accountability, leadership selection, and safe randomness generation. The framework for accountable and reconfigured distributed systems enables seamless adaptation in response to failures using lattice agreement abstraction. In addition, innovative cryptographic protocols improve leadership elections on partially synchronous blockchains, improving consensus mechanisms and system resilience [15]. As distributed systems increasingly rely on log-based monitoring to assess security, the reliability of deep learning models against malicious attacks is a growing concern. A new attack method, LAM, manipulates streaming logs to avoid detecting anomalies, highlighting the need for enhanced security measures against adversarial manipulation [16].

Security policies in distributed systems also need to be flexible and validated in different implementations. A language-independent policy review system ensures compliance with security policies by analyzing I/O behavior instead of relying on programming language restrictions. Evaluations demonstrate its applicability in real-world protocols, which reinforces the need for adaptive security policies [17]. Blockchain technology also contributes to cybersecurity by increasing the transparency and security of data in distributed governance systems. However, issues such as scalability and interoperability must be addressed in order to fully exploit the potential of blockchain to protect sensitive data [18]. Finally, advances in deep learning to detect anomalies in distributed system logs introduce models that integrate global spatiotemporal features, greatly improving the accuracy of detecting security threats in complex environments [19]. These changes combine to contribute to the reliability and effectiveness of cybersecurity assessments in corporate networks.

Cybersecurity assessments in corporate networks must constantly adapt to changing threats and technological advancements. Distributed systems and computational approaches, including blockchain technology and distributed ledgers, offer significant potential to improve financial crime prevention and cybersecurity by increasing transparency and reducing fraud risks. However, issues such as regulatory compliance, interoperability, and integration with existing infrastructures must be addressed to maximize these benefits [20]. A proactive approach to security is essential in distributed environments, and the integration of DevOps methodologies enhances security by embedding threat detection into the development lifecycle, automating monitoring, and using behavioral analytics to detect anomalies in real-time. This strategy contributes to the formation of a culture of shared responsibility for safety and compliance with legal standards [21].

The diversity of systems is another key factor in improving the reliability and security of distributed communication networks. Analytical models based on tension-force analysis quantify these improvements, providing valuable information about the stability of the system [22]. In the context of intelligent distributed systems (SDS), ensuring data security and interoperability is critical for the seamless exchange of information between industries such as healthcare, utilities, and supply chains. Setting global security standards can provide a framework for authentication, collaboration, and protection against cyber threats in SDS environments [23]. The growing integration of IoT with cloud computing introduces new vulnerabilities, requiring a comprehensive security framework that increases resilience to cyber threats while maintaining scalability and adaptability in distributed environments [24].

Data privacy remains a major concern, especially in areas such as education and healthcare. Distributed computing offers improvements in security and response times, however, centralized platforms often outperform distributed systems with privacy-preserving techniques such as k-anonymity, t-proximity, and β-probability. Comparative analysis of these approaches reveals trade-offs in runtime, memory requirements, and suppression levels [25]. In healthcare, foggy computing is a promising solution for real-time patient monitoring, but security and privacy concerns must be addressed through encryption, access control, and data analysis techniques that preserve privacy [26]. Risk assessment in distributed information systems requires a dynamic, multi-layered approach that integrates quantitative, qualitative, and hybrid methodologies, using security metrics for accurate and reliable cybersecurity assessments [27].

Cybersecurity threats in smart networks highlight the importance of advanced threat detection mechanisms. Traditional supervised learning methods for detecting cyberattacks require a variety of training datasets that may not always be available. Unsupervised data mining approaches, especially for detecting false data attacks (FDIA), offer a more efficient alternative, relying solely on conventional event data to train detection models. Comparative studies demonstrate that unsupervised algorithms are superior to supervised and deep learning methods in detecting unknown attack patterns, increasing cybersecurity in smart grid infrastructures [28].

These advances combine to strengthen cybersecurity assessment systems in corporate networks, ensuring resilience to sophisticated cyber threats. Cybersecurity assessments in corporate networks should include advanced cryptographic techniques to reduce the risks of data breaches in distributed environments. Cloud cryptography plays

a crucial role in protecting data storage and transmission through the use of encryption mechanisms, intrusion detection systems, and firewalls. These technologies strengthen data protection in cloud-based distributed systems, preventing unauthorized access and infiltration of malware [29]. With the expansion of cloud and edge computing, AI-powered forensic tools have become effective solutions for detecting and mitigating the effects of cyber incidents in real-time. Machine learning and deep learning techniques improve forensic analysis by improving scalability, accuracy, and response time when detecting cyber threats in distributed systems [30].

The function for evaluation fo cybersecurity of computer stations

Let's set two functions to assess the level of network security, where the first will reflect the likelihood of significant interference of an attacker in any critical component of the network.

First, let's define the vulnerability of a component as the probability of its compromise regardless of the rest present in the network. Corresponding formula is:

$$V = \omega_S S + \omega_P(1 - P) + \omega_U U, \tag{1}$$

where S is the software vulnerability level in range [0,1], P is the effectiveness of cybersecurity policies in range [0, 1], 1 standing for maximal security, U – probability of compromise due to a human error, $\omega_S, \omega_P, \omega_U$ are the weight coefficients.

Let's reveal the components of the formula further. P should be defined by cybersecurity professionals independently on a case-by-case basis, as different organizations have different approaches to setting up appropriate processes. In the context of this work, we will determine U according to the frequency of phishing attacks and other situations of compromise of network users in its history. S will be determined by the formula

$$S = \sum_{k=1}^{N_e} \omega_k * \frac{CVSS_k}{10}, \tag{2}$$

where N_e is the total number of vulnerabilities on the node, $CVSS_k$ is the assessment of the criticality of the k-th vulnerability on the CVSS scale (from 0 to 10), ω_k is the weighting coefficient, which determines the impact of each vulnerability.

Vulnerability search for S calculation can be organized using vulnerability scanners. Thus, the formula for the vulnerability of one component independently of the rest of the network:

$$V = \omega_S \sum_{k=1}^{N_e} \omega_k * \frac{CVSS_k}{10} + \omega_P(1 - P) + \omega_U U, \tag{3}$$

It should also be borne in mind that the compromise of one host in the network also endangers other components of the network. To do this, we will specify a formula to determine the probability of compromise of host j if host i was compromised:

$$G_{ij} = \omega_T T_{ij} + \omega_F(1 - F_{ij}) + \omega_L(1 - L_{ij}), \tag{4}$$

where T_{ij} is the the level of connection openness normalized in the range [0,1], where 1 means a fully open channel and 0 is a fully isolated connection, F_{ij} is the effectiveness of firewalls and traffic filtering (from 0 to 1, where 1 means maximum protection), L_{ij} is the encryption level (0 to 1, where 1 means full encryption and 0 means fully open traffic).

Let's put these two formulas together to determine the probability of its compromise for each host and, accordingly, calculate the chance of compromise of any of the important hosts.

$$CS = \prod_{i=1}^{M} \left(\left(1 - V_{a_i}\right) * \prod_{j=1}^{N} \left(1 - V_j P_{a_i}\right) \right), \tag{5}$$

where CS is the overall level of cybersecurity in the corporate network, M is the number of important network components, a is the list of important network components.

These formulas are based on comprehensive mathematical modeling that adequately accounts for both the internal characteristics of each host and the interdependencies between them. The vulnerability level of each node V is determined by three key parameters: software vulnerabilities S, the effectiveness of security policies P, and the probability of compromise due to human factors U. This structure aligns with modern cybersecurity threat analysis practices, where most incidents stem not only from technical flaws but also from social engineering and imperfect security administration. The use of weighting coefficients enables the model to reflect the relative importance of each factor in a given context, making the evaluation adaptable to the specific conditions of the network.

Further modeling of the probability of attack propagation across the network through the function $G(i, j)$ captures the probabilistic nature of inter-node interaction, where the risk of transmission depends on parameters such as connection openness, firewall effectiveness, encryption levels, and anomaly detection capabilities. This

formula is crucial, as it accounts for not only the vulnerability of individual components but also their potential influence on other nodes—an essential distinction from traditional approaches that treat hosts in isolation.

The final stage involves the calculation of the overall cybersecurity level of the network CS, which is derived by combining all obtained V and G values. The formula for CS implements a multiplicative scheme that accurately reflects the cumulative nature of risks: even if a single host is highly vulnerable and located in a poorly protected segment, it can impact the security of the entire system. This approach allows for the estimation of the probability of a successful attack not only on isolated components but on critical infrastructure as a whole.

Taken together, the proposed formulas are not only mathematically sound but also effective in addressing the task of constructing a comprehensive cybersecurity evaluation model for corporate networks. They provide a high degree of accuracy, adaptability to changes in system configuration, and the ability to tailor to specific threats and architectures, making the proposed methodology universally applicable across a wide range of practical implementations.

Practical implementation of the system

The method for synthesizing self-organizing systems for cybersecurity assessment of computer stations is based on constructing a system capable of real-time monitoring of the corporate network and individual computer stations. It continuously collects relevant metrics and computes a cybersecurity evaluation function. The central element of this system is a function that reflects the current level of protection of the information infrastructure, taking into account numerous interdependent factors. This function should be formed based on aggregated indicators of system process activity, configuration integrity, network connection status, and the degree of vulnerability derived from known technical software characteristics and the enforcement level of access control policies.

To deploy the evaluation system, an initial configuration of coefficients and values is required—parameters that cannot be accurately assessed using purely technical methods. Let us now consider Formula 3, which calculates the vulnerability of each individual computer in the network:

$$V = \omega_S \sum_{k=1}^{N_e} \omega_k * CVSS_k + \omega_P(1-P) + \omega_U U$$

In this formula, the weighting coefficients $\omega_S, \omega_P, \omega_U$, as well as the values of P and U under ideal circumstances, should be determined by cybersecurity experts for each specific case of a corporate network. This approach assumes individual customization of the evaluation system, taking into account the architecture's specifics, the types of information assets, the organizational structure of the enterprise, as well as the potential attack vectors characteristic of a particular industry or region. Alternatively, the following values for the weighting coefficients are proposed:

Network Scenario	ω_S	ω_P	ω_U
Techno-centric organization	0.7	0.2	0.1
Institution with a bureaucratic structure	0.2	0.5	0.3
Company under active phishing conditions	0.3	0.2	0.5

Similarly, the values P and U should also be determined by cybersecurity experts (ideally) based on an audit that demonstrates the network's security policies comply with the latest standards and that personnel are knowledgeable and proficient in computer usage. Alternatively, the value of P can be roughly estimated based on components such as the existence of documented security policies, the currency of the policies, access control, password management, and incident response. Likewise, the value of U can be approximated based on other factors and historical data: the frequency of phishing incidents over the past year, the level of personnel awareness (tests/surveys), the availability of regular training, incidents of password/access loss, and the results of social engineering simulations.

To determine the remaining values in the formula ($\omega_k, N_e, CVSS_k$) specialized software and additional resources are required. To obtain $CVSS_k$, it is recommended to use the OpenVAS vulnerability scanner. This is a free and open-source software – which ensures there is no misuse of network access by the developers – provided that changes to the open code are regularly reviewed. For the cybersecurity evaluation system to function properly, it is necessary to regularly run vulnerability scans on the computer. As a result of these scans, the program generates a report, and the CVSS values extracted from it will be used for further calculations.

To determine ω_k, N_e , it is proposed to use daily updated data from the Exploit Prediction Scoring System (EPSS) model. This is a system that estimates the probability that a specific vulnerability will be exploited in the real world within the next 30 days. Data can be obtained via API or by downloading reports in CSV format. Each row in the file is a triplet: CVE (vulnerability identifier), EPSS (probability of exploitation), Percentile (probability percentile for the given vulnerability). N_e will be taken as the number of vulnerabilities in the EPSS report, and ω_k –

$EPSS_k$, normalized in such a way that the sum of all values equals one. In this way, the weight of a vulnerability will be proportional to the probability of encountering it.

Let us consider formula 4:

$$G_{ij} = \omega_T T_{ij} + \omega_F(1 - F_{ij}) + \omega_L(1 - L_{ij}) + \omega_D(1 - D_{ij}),$$

where T_{ij} is the level of openness within the range [0, 1], F_{ij} is the effectiveness of firewalls and traffic filtering within the range [0, 1], L_{ij} is the level of encryption within the range [0, 1], D_{ij} is the level of anomaly detection within the range [0, 1], $\omega_T, \omega_F, \omega_L, \omega_D$ – the weighting coefficients.

The weighting coefficients $\omega_T, \omega_F, \omega_L, \omega_D$ should be defined by the CISO (Chief Information Security Officer) or a security analyst. For example, in a cloud environment with many open ports but strong encryption – more weight should be assigned to ω_T, and less to ω_L, whereas in an environment without IDS/IPS (Intrusion Detection/Prevention Systems) – ω_D should be increased.

This can be implemented in the form of a risk profile table:

Scenario	ω_T	ω_F	ω_L	ω_D
Cloud infrastructure	0.1	0.5	0.2	0.2
Corporate local network	0.1	0.4	0.3	0.2
Minimal access control	0.1	0.2	0.1	0.4

It is also necessary to define $T_{ij}, F_{ij}, L_{ij}, D_{ij}$. Let us calculate T_{ij}:

$$T_{ij} = \frac{N_o}{N_a}, \quad (4.1)$$

where N_o is the number of open ports excluding standard encrypted ones (e.g., HTTPS), and N_a is the maximum allowable number of open ports, typically set to 10.

Let us calculate F_{ij}. This is done through periodic active testing – by generating requests that simulate malicious traffic. It is recommended to use the open-source tool hping to generate such traffic. The formula is:

$$F_{ij} = \frac{N_{failed}}{N_{tests}}, \quad (4.2)$$

where N_{failed} is the number of malicious test requests that were not blocked during testing, and N_{tests} – is the total number of tests conducted.

Let us calculate L_{ij}. It is proposed to use the tool SSLyze to scan network connections and assess the strength of encryption. Based on the scan results, a numerical value can be estimated for use in formula (4). Since TLS 1.3 is currently considered the most secure transport layer encryption protocol, it is rated as $L_{ij} = 1$. SSL, being outdated and known to contain vulnerabilities, is rated as $L_{ij} = 0$. . For intermediate values, we assign $L_{ij} = 0.7$ for TLS 1.2 and $L_{ij} = 0.3$ for TLS 1.1.

Results of the experiment

To evaluate the effectiveness of the proposed model, an experiment was conducted that simulates the operation of the implemented cybersecurity assessment system under conditions close to a real-world environment. The testing involved simulating the activity of network nodes over the course of one week with an hourly time step. During the experiment, dynamic updates of input parameters were implemented – these parameters influence the vulnerability level of individual computers and the probability of their compromise as a result of interaction with other nodes in the network.

The model components responsible for forming the vulnerability and compromise probability functions were manually configured based on assumptions about the typical characteristics of an organizational IT environment. In particular, the weight coefficients for the technical, policy-related, and human vulnerability components were set according to conditionally prioritized security concerns. Similarly, the weights for traffic, filtering, encryption, and network remoteness parameters were chosen to reflect the characteristic risks of network intrusion through interactions between individual computers. The values of the manually configured parameters are as follows: $\omega_S = 0.7, \omega_P = 0.2, \omega_U = 0.1, \omega_T = 0.1, \omega_F = 0.4, \omega_L = 0.3, \omega_D = 0.2, P = 0.9, U = 0.1$.

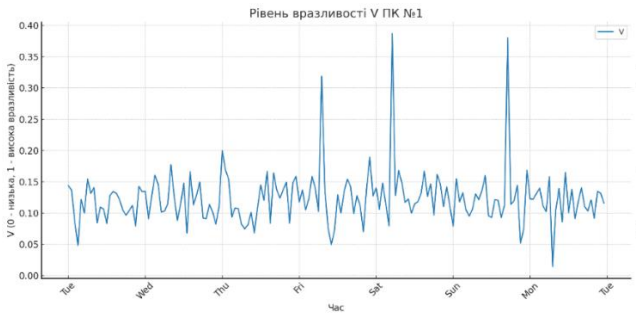


Fig. 1

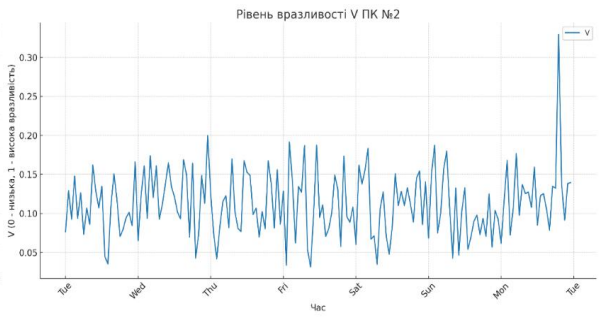


Fig. 2

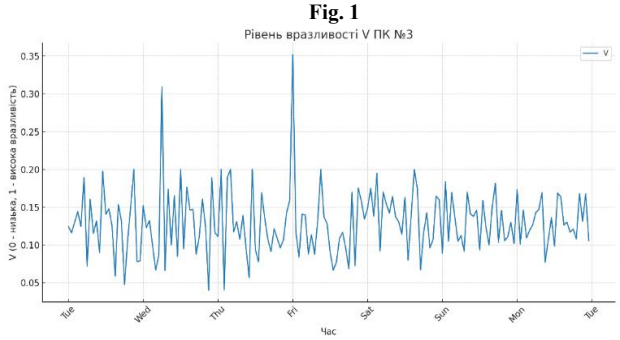


Fig. 3

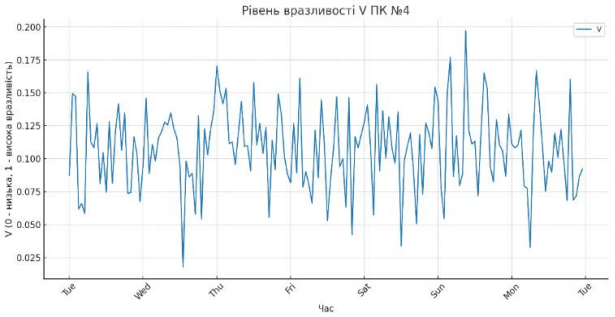


Fig. 4

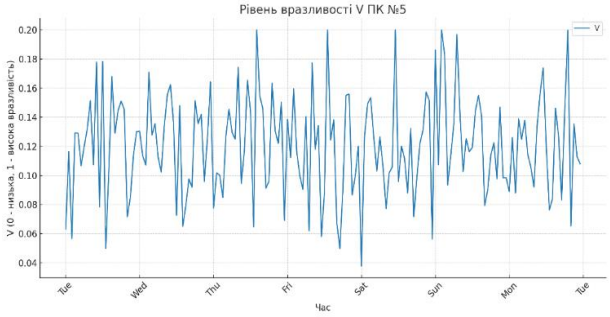


Fig. 5

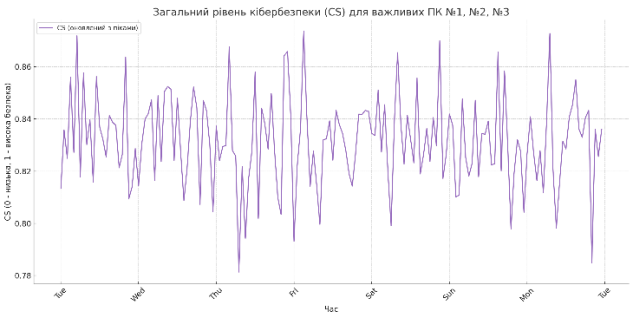


Fig. 6

As part of the experiment, isolated peak deviations were manually introduced for critical nodes – computers No. 1-3, – simulating episodic increases in risk level. These peaks were implemented by artificially adding a noticeable number of high-rated technical vulnerabilities, equivalent to a situation where a new set of critical vulnerabilities is discovered on a specific host, for example, due to a missed update or newly identified software flaws. As a result, there were short-term but sharp increases in the V indicator, which are clearly visible in Fig. 1–3. Fig. 4-5 show vulnerability chart with no serious peaks.

The chart of the overall cybersecurity level CS (Fig. 6) serves as a key analytical tool that enables a comprehensive assessment of the security situation within the network, taking into account both the local characteristics of individual nodes and the impact of inter-node interactions. The construction of this indicator is based on integrating the vulnerability assessments of critical computers with the probabilities of their compromise by other elements of the system. This approach provides a multidimensional view of risks, allowing not only for isolated evaluations of individual hosts but also for tracking systemic dependencies and potential attack chains.

This chart holds particular value from the perspective of real-time monitoring – it makes it possible to identify critical time intervals during which a sharp decline in the security level is observed, and to correlate these changes with specific hosts exhibiting increased vulnerability or an escalating threat of compromise. In combination with the V_i graphs, which provide detailed insight into the sources of these changes, the CS graph enables the operator to instantly assess the overall network situation, localize problem areas, and take timely measures to eliminate vulnerabilities or reduce the risk of attack propagation.

Thus, CS visualization serves as an effective real-time decision-making mechanism, which is especially important in the context of a rapidly changing threat landscape. Its integration into the security management system significantly enhances the response speed and the rationality of actions taken by the administrator or automated defense systems.

Conclusions

The proposed system for cybersecurity evaluation of corporate networks effectively integrates technical, organizational, and human factors into a comprehensive framework. By employing adaptive mathematical modeling

and real-time data analysis, it provides an accurate, dynamic assessment of a network's security posture. The approach's strength lies in its flexibility—allowing parameter customization based on the specifics of an organization—and its capability to evaluate not only isolated vulnerabilities but also interdependencies between network nodes. Experimental implementation demonstrated the model's practical applicability and its usefulness for identifying weak points, prioritizing response measures, and enhancing decision-making in security management. This system represents a significant step forward in proactive cybersecurity assessment, offering organizations a scalable and intelligent tool to fortify their digital infrastructure against evolving threats.

References

1. Savenko B., Kashtalian A., Lysenko S., Savenko O. Malware Detection By Distributed Systems with Partial Centralization. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany.* 2023. 265–270. https://doi.org/10.1109/IDAACS58523.2023.10348773
2. Kashtalian A., Lysenko S., Savenko O., Nicheporuk A., Sochor T., Avsiyevych V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems.* 2024. No. 1, 152–175. https://doi.org/10.32620/reks.2024.1.13
3. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A. Self-adaptive System for the Corporate Area Network Resilience in the Presence of Botnet Cyberattacks. *Computer Networks. CN 2018. Communications in Computer and Information Science,* Vol. 860. 2018. https://doi.org/10.1007/978-3-319-92459-5_31
4. Savenko O., Sachenko A., Lysenko S., Markowsky G., Vasylkiv N. Botnet Detection Approach Based on the Distributed Systems. *International Journal of Computing.* 2020. Vol. 19(2), 190–198. https://doi.org/10.47839/ijc.19.2.1761
5. Yadav A., Kaur M., Sharma C., Prashar D. Next-gen distributed denial-of-service detection and mitigation in software-defined networking using hybrid machine learning approach. *Soft Computing in Smart Manufacturing and Materials.* 2025. 97–133. https://doi.org/10.1016/B978-0-443-29927-8.00005-9
6. Liu Y., Ren S., Wang X., Zhou M. Temporal Logical Attention Network for Log-Based Anomaly Detection in Distributed Systems. *Sensors.* 2024. Vol. 24. https://doi.org/10.3390/s24247949
7. Chaurasia B., Verma A., Verma P. An in-depth and insightful exploration of failure detection in distributed systems. *Computer Networks.* 2024. Vol. 247. https://doi.org/10.1016/j.comnet.2024.110432
8. Wei X., Wang J., Sun C., Towey D., Zhang S., Zuo W., Yu Y., Ruan R., Song G. Log-based anomaly detection for distributed systems: State of the art, industry experience, and open issues. *Journal of Software: Evolution and Process.* 2024. Vol. 36(8). https://doi.org/10.1002/smr.2650
9. Vankayalapati R.K. Zero-Trust Security Models for Cloud Data Analytics: Enhancing Privacy in Distributed Systems. *SSRN.* 2025. https://doi.org/10.2139/ssrn.5121185
10. Di Pilla P., Pareschi R., Salzano F., Zappone F. Listening to what the system tells us: Innovative auditing for distributed systems. *Frontiers in Computer Science.* 2022. Vol. 4. https://doi.org/10.3389/fcomp.2022.1020946
11. Botha-Badenhorst D., McDonald A.M., Barbour G.D., Buckinjohn E., Gertenbach W. On The Zero-Trust Intranet Certification Problem. *Proceedings of The 19th International Conference on Cyber Warfare and Security.* 2024. Vol. 19(1). https://doi.org/10.34190/iccws.19.1.2054
12. Wang Y., Yang X. Design and implementation of a distributed security threat detection system integrating federated learning and multimodal LLM. *arXiv.* 2025. https://doi.org/10.48550/arXiv.2502.17763
13. Zhang H., Jia X., Chen C. Deep Learning-Based Real-Time Data Quality Assessment and Anomaly Detection for Large-Scale Distributed Data Streams. *International Journal of Medical and All Body Health Research.* 2025. Vol. 6(1). https://doi.org/10.54660/IJMBHR.2025.6.1.01-11
14. Wang B., He Y., Shui Z., Xin Q., Lei H. Predictive optimization of DDoS attack mitigation in distributed systems using machine learning. *Applied and Computational Engineering.* 2024. Vol. 64(1), 89–94. https://doi.org/10.54254/2755-2721/64/20241350
15. Freitas de Souza L. Achieving accountability, reconfiguration, randomness, and secret leadership in byzantine fault tolerant distributed systems. *Distributed, Parallel, and Cluster Computing [cs.DC], Institut Polytechnique de Paris.* 2024. URL: https://hal.science/tel-04984550 (access date: 21.01.2025)
16. Herath J.D., Yang P., Yan G. Real-Time Evasion Attacks against Deep Learning-Based Anomaly Detection from Distributed System Logs. *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21).* 2021. 29–40. https://doi.org/10.1145/3422337.3447833
17. Wolf F.A., Müller P. Verifiable Security Policies for Distributed Systems. *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24).* 2024. 4–18. https://doi.org/10.1145/3658644.3690303
18. Chandan R.R., Torres-Cruz F., Figueroa E.N.T., Mendoza-Mollocondo C.I., Sisodia D.R., Alam T., Tiwari M. Revolutionizing Data Management and Security with the Power of Blockchain and Distributed System. *Meta Heuristic Algorithms for Advanced Distributed Systems.* 2024. Chapter 11. https://doi.org/10.1002/9781394188093.ch11
19. Han P., Li H., Xue G., Zhang C. Distributed system anomaly detection using deep learning-based log analysis. *Computational Intelligence.* 2023. Vol. 39(3), 433–455. https://doi.org/10.1111/coin.12573
20. Singh V.B.P., Singh P., Guha S.K., Shah A.I., Samdani A., Nomani M.Z.M., Tiwari M. The Future of Financial Crime Prevention and Cybersecurity with Distributed Systems and Computing Approaches. *Meta Heuristic Algorithms for Advanced Distributed Systems.* 2024. Chapter 19. https://doi.org/10.1002/9781394188093.ch19
21. Allam A.R. Enhancing Cybersecurity in Distributed Systems: DevOps Approaches for Proactive Threat Detection. *Silicon Valley Tech Review.* 2023. Vol. 2(1), 54–66. URL: https://www.researchgate.net/publication/385886881_Enhancing_Cybersecurity_in_Distributed_Systems_DevOps_Approaches_for_Proactive_Threat_Detection (access date: 21.01.2025)
22. Popov G., Popova A. Application of System Diversity for Increasing Security and Reliability of Distributed Systems. *2022 XXXI International Scientific Conference Electronics (ET), Sozopol, Bulgaria.* 2022. 1–4. https://doi.org/10.1109/ET55967.2022.9920304
23. Maher D.P., Ahatlan H.E., Poonegar A.D. A Standardized Trust Model for Enabling Data Security and Interoperability within Smart Distributed Systems. *2023 IEEE International Smart Cities Conference (ISC2), Bucharest, Romania.* 2023. 1–4. https://doi.org/10.1109/ISC257844.2023.10293630
24. Raja M. Comprehensive Framework for Secure Cloud Computing and Distributed Systems with Integrated Cybersecurity and Information Assurance in the Era of Internet of Things. *International Journal of Information Technology Research and Development (IJITRD).* 2025. Vol. 6(2), 7–16. URL: https://ijitrd.com/index.php/home/article/view/IJITRD_6_2_2 (access date: 21.01.2025)
25. Lamaazi H., Alneyadi A.M.M., Serhani M.A. Academic Data Privacy-Preserving using Centralized and Distributed Systems: A Comparative Study. *Proceedings of the 2024 6th International Conference on Big-data Service and Intelligent Computation (BDSIC '24).* 2024. 8–16. https://doi.org/10.1145/3686540.3686542

26. Arora D., Sharma O. Fog Computing in Healthcare: Enhancing Security and Privacy in Distributed Systems. *Artificial Intelligence and Cybersecurity in Healthcare.* 2025. Chapter 3. https://doi.org/10.1002/9781394229826.ch3

27. Palko D., Babenko T., Bigdan A., Kiktev N., Hutsol T., Kuboń M., Hnatiienko H., Tabor S., Gorbovy O., Borusiewicz A. Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences.* 2023. Vol. 13(4), 2393. https://doi.org/10.3390/app13042393

28. Pinto S.J., Siano P., Parente M. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies.* 2023. Vol. 16(4), 1651. https://doi.org/10.3390/en16041651

29. Dubey H., Kumar S., Chhabra A. Cyber Security Model to Secure Data Transmission using Cloud Cryptography. *Cyber Security Insights Magazine.* 2022. Vol. 2. URL: https://insights2techinfo.com/wp-content/uploads/2022/11/Cyber-Security-Model-to-Secure-Data-Transmission-using-Cloud-Cryptography_final_2.pdf (access date: 21.01.2025)

30. Kyle J., Alexander D. AI-Driven Forensic Tools for Cloud and Edge Computing. *International Journal of Computational Intelligence in Digital Systems.* 2022. Vol. 11(1), 29–45. URL: https://www.researchgate.net/publication/388494481_AI-Driven_Forensic_Tools_for_Cloud_and_Edge_Computing (access date: 21.01.2025)

Ihor Ramskyi **Ігор Рамський**	Master's degree student, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: ramskyihor@gmail.com https://orcid.org/0009-0007-6175-1923	Магістрант, Хмельницький національний університет
Andriy Drozd **Андрій Дрозд**	PhD student, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: andriydrozdit@gmail.com https://orcid.org/0009-0008-1049-1911	Аспірант, Хмельницький національний університет
Oleksii Lyhun **Олексій Лигун**	PhD student, Khmelnytskyi National University, Khmelnytskyi, Ukraine e-mail: oleksii.lyhun@gmail.com https://orcid.org/0009-0004-5727-5096	Аспірант, Хмельницький національний університет

https://doi.org/10.31891/csit-2025-2-15
UDC 004.93:94

BIERIESTOVA Mariia, MOROZ Volodymyr
Odesa National University

IDENTIFICATION OF SOUNDS BASED ON THE HILBERT-HUANG TRANSFORM FOR THE TASK OF DETECTING UAVs

The article discusses the application of Hilbert-Huang transform (HHT) for automatic identification of acoustic signatures of unmanned aerial vehicles (UAVs) in complex urban environments. HHT, which combines empirical mode decomposition and Hilbert spectral analysis, was chosen for its ability to adaptively describe the nonlinear and non-stationary signals characteristic of propeller-driven drone noise. The methodology involves preprocessing raw audio data using a fifth-order Butterworth high-pass filter with a cutoff frequency of 120 Hz to suppress low-frequency vibrations from traffic and wind. Each three-second segment is further segmented into 30-millisecond frames with 10 ms hop (≈ 33 % overlap), giving sufficient temporal resolution while preserving quasi-stationarity. Each frame is pre-whitened using a discrete cosine transform: the energy spectrum is smoothed, emphasizing local propeller harmonics. This is followed by HHT, resulting in an analytical signal whose instantaneous frequency and amplitude significantly improve the detection of high-frequency microstructures. 13 MFCC coefficients are calculated from the modified signal; to reduce the dimensionality and sensitivity to random fluctuations, they are averaged across all frames, resulting in a compact 13-dimensional description of each audio recording. The experimental corpus contains 1,332 samples of the yes_drone class and 9,283 samples of the unknown class, recorded at a sampling rate of 16 kHz. A two-layer perceptron with 64 and 32 neurons was used for training, which uses ReLU activation and ends with a sigmoid node that generates the probability of a signal belonging to the "drone" class. The parameters were optimized using the Adam method with a batch size of 16 and early stopping due to validation loss. On the held-out test subset, the model achieves an overall accuracy of 0.94; yes_drone recall is 0.83, and unknown F1 is 0.96, giving false-alarm performance comparable to the MFCC + SVM baseline. The HHT remains competitive with deep CNNs in accuracy while running far faster: processing a 3-s file takes ≈ 0.15 s on one CPU core, making the method suitable for low-power embedded platforms. Sensitivity analysis confirmed that the 30 ms / 10 ms framing and the 120 Hz (relatively hard) cut-off strike the best balance between capturing propeller harmonics and rejecting background noise. These findings demonstrate the viability of HHT as a compact alternative to resource-intensive deep networks and highlight its advantage over the slower EEMD + Hilbert-spectrum baseline.

Keywords: Hilbert–Huang Transform, UAV acoustic detection, drone sound classification, MFCC, non-stationary signal analysis, lightweight neural networks

БЄРЄСТОВА Марія, МОРОЗ Володимир
Одеський національний університет

ІДЕНТИФІКАЦІЯ ЗВУКІВ НА ОСНОВІ ПЕРЕТВОРЕННЯ ГІЛЬБЕРТА-ХУАНГА ДЛЯ ЗАДАЧІ ВИЯВЛЕННЯ БПЛА

У роботі досліджується застосування перетворення Гільберта–Хуанга (HHT) для задачі автоматичної ідентифікації акустичних сигнатур безпілотних літальних апаратів (БПЛА) у складному фоні міського середовища. HHT, що поєднує емпіричне модове розкладання та спектральний аналіз Гільберта, обрано через його здатність адаптивно описувати нелінійні та нестаціонарні сигнали, властиві шуму гвинтомоторної групи дронів. Методологія передбачає попередню обробку сирих аудіоданих високочастотним фільтром Баттерворта п'ятого порядку зі зрізом 120 Гц для придушення низькочастотних вібрацій дорожнього руху й вітру. Кожен трисекундний відрізок далі сегментується на 30-мс фрейми з кроком 10 мс (≈ 33 % перекриття), що забезпечує достатню часову роздільну здатність і водночас зберігає стаціонарність усередині вікна. До кожного фрейма застосовується попереднє «вибілювання» шляхом дискретного косинусного перетворення: енергетичний спектр нівелюється, акцентуючи локальні гармоніки пропелерів. Після цього виконується HHT, за підсумком якого формується аналітичний сигнал, чия миттєва частота й амплітуда суттєво покращують виявлення високочастотних мікроструктур. Із модифікованого сигналу обчислюються 13 коефіцієнтів MFCC; для зменшення розмірності та зниження чутливості до випадкових флуктуацій їх усереднюють по всіх фреймах, отримуючи компактний 13-вимірний опис кожного аудіозразка. Експериментальний корпус містить 1,332 семплів класу yes_drone та 9,283 семплів unknown, записаних з частотою дискретизації 16 кГц. Для навчання використано двошаровий персептрон із 64 та 32 нейронами, що застосовує ReLU-активацію й завершується сигмоїдним вузлом, який генерує ймовірність належності сигналу до класу «дрон». Параметри оптимізовано методом Adam при батч-розмірі 16 та ранній зупинці за валідаційною втратою. На відкладеній тестовій підмножині модель досягає загальної точності 0.94; показник recall для yes_drone становить 0.83, а F1-оцінка класу unknown — 0.96, що свідчить про низьку частоту хибних спрацювань порівняно з базовим MFCC+SVM. HHT-підхід наближається до глибоких CNN-моделей за точністю, проте значно перевершує їх за швидкістю й обчислювальною ефективністю: обробка триває ≈ 0.15 с на ядро CPU без GPU, що робить алгоритм придатним для енергообмежених вбудованих платформ. Аналіз чутливості підтвердив, що 30 мс / 10 мс та зріз 120 Гц забезпечують найкращий баланс між виділенням пропелерних гармонік і придушенням фону. Отримані результати демонструють життєздатність HHT як компактної та ефективної альтернативи ресурсомістким глибоким мережам, відкриваючи шлях до легких сенсорних вузлів протидії БПЛА у реальному часі. Також проведено порівняння з алгоритмом EEMD + Hilbert-spectrum statistics.

Ключові слова: перетворення Гільберта–Хуанга, акустичне виявлення БПЛА, класифікація звуку дрона, MFCC, аналіз нестаціонарних сигналів, полегшені нейронні мережі

Introduction

In modern situational-awareness systems, one of the most pressing and technically demanding tasks is the automatic detection and classification of acoustic signatures emitted by unmanned aerial vehicles (UAVs). The

performance of such systems is critical to infrastructure security, yet researchers face numerous challenges that call for novel approaches capable of improving accuracy and processing speed under highly dynamic acoustic conditions.

Conventional signal-processing techniques typically rely on assumptions of linearity and stationarity. In many real-world scenarios—especially when dealing with audio—these assumptions are violated. Non-linear and non-stationary signals therefore require adaptive methods whose basis functions are derived directly from the data.

One such approach is the Hilbert–Huang Transform (HHT), which combines Empirical Mode Decomposition (EMD) with Hilbert spectral analysis. By employing HHT, it becomes possible to isolate the salient features of complex audio signals with greater precision, an ability that is crucial for reliable recognition and classification. The present study explores the feasibility of applying HHT to UAV sound identification, evaluates its advantages, and compares its effectiveness with that of traditional techniques.

Related works

Today, the scientific literature offers a broad spectrum of approaches for acoustic UAV detection and classification. Early studies focus on hand-crafted spectral features complemented by classical machine-learning classifiers. Mrabet et al. [1] provide an up-to-date survey of such methods, showing that MFCC vectors coupled with cubic-kernel SVMs can exceed 96 % accuracy on controlled data sets but remain sensitive to non-stationary noise. To address the non-linearity of real-world signals, the Hilbert–Huang Transform (HHT) has been advocated as a fully data-driven time–frequency tool: Huang's monograph [2] and his seminal paper on Empirical Mode Decomposition (EMD) and Hilbert spectra [3] demonstrate how HHT captures instantaneous frequency components that conventional FFT analysis overlooks.

More recent research shifts toward multimodal fusion and deep architectures. Kim et al. [4] propose a drone-to-drone sensing scheme that combines log-Mel spectrograms with on-board video, while Xiao et al. [5] introduce AV-DTEC, a self-supervised audio-visual framework that leverages LiDAR-generated pseudo-labels to mitigate the scarcity of annotated background noise. Parallel efforts aim at reducing model complexity for edge deployment: Aydın and Kızılay [6] design a light-weight CNN that detects amateur drones under harsh acoustic conditions with minimal computational overhead.

Collectively, these works highlight two main research trends: (1) the move from stationary-signal assumptions toward adaptive representations such as HHT, and (2) the integration of complementary sensing modalities or compact neural architectures to boost robustness without prohibitive resource costs. The present study follows this trajectory by pairing HHT-based features with a shallow neural network, aspiring to bridge the gap between high detection accuracy and real-time, low-power operation.

Experimental Methodology

Experimental verification was carried out on a binary corpus of real field recordings containing 1332 samples of the yes_drone class and 9283 samples of the unknown class. All computations were performed in Python 3.12 with the scientific stack (NumPy, SciPy, librosa, TensorFlow).

Each waveform *x(t)* was first passed through a fifth-order Butterworth high-pass filter

$$|H(\omega)|^2 = \frac{\omega^{10}}{\omega^{10} + \omega_c^{10}},$$

where the cut-off frequency $\omega_c = 2\pi f_c$ was swept in the range $f_c \in \{80, 100, 120\}$ Hz during hyper-parameter search. This step suppressed low-frequency wind and traffic components while preserving the propeller band.

The filtered signal was then segmented into frames of length $L \in \{20, 25, 30\}ms$ with hops $H \in \{10, 12.5, 15\}ms$ $(40 - 50\%\ overlap)$. Each frame $x_n[k]$ was windowed by a Hamming function

$$\omega[k] = 0.54 - 0.46\cos\left(\frac{2\pi k}{L-1}\right), \quad 0 \le k \le L,$$

to minimise spectral leakage.

For every windowed frame $s_n[k] = x_n[k] \cdot \omega[k]$ the discrete cosine transform

$$S_n[m] = \sum_{k=0}^{L-1} s_n[k]\, cos\left[\frac{\pi}{L}(k + \frac{1}{2})m\right], \quad 0 \le m < L,$$

acts as a spectral equaliser, concentrating energy in the first coefficients and reducing autocorrelation.

The DCT sequence is converted into an analytic signal via a modified FFT scheme:

$$\widetilde{S_n}[m] = \begin{cases} S_n[m], & m = 0\ or\ m = L/2 \\ 2S_n[m], & 1 \le m < L/2 \\ 0, & L/2 < m < L \end{cases}$$

Applying the inverse FFT yields

$z_n[k] = F^{-1}\{\widetilde{S_n}[m]\} = a_n[k]e^{j\varphi_n[k]},$

whose modulus $a_n[k]$ captures the instantaneous high-frequency components characteristic of rotor noise.

From $a_n[k]$ we compute 13-Mel-frequency cepstral coefficients:

$$MFCC_n[p] = \frac{1}{M}\sum_{m=1}^{M} \log(E_n[m]) \cos\left[\frac{\pi}{M}\left(m-\frac{1}{2}\right)p\right],$$

with *M* mel filters and *p=0,…,12*. Here $E_n[m]$ denotes filter-bank energies obtained with parameters *n_fft=L, hop_length>L* so that each frame contributes exactly one coefficient vector. Averaging over all frames in a file gives a 13-dimensional feature vector $\bar{c}$.

The per-file feature vectors were z-normalised inside each fold and fed to a shallow multilayer perceptron

$y = \sigma(W_2 ReLU(W_1\bar{c} + b_1) + b_2)$,

where $W_1 \in \mathbb{R}^{64\times13}$ and $W_2 \in \mathbb{R}^{32\times64}$.

Training details:

Loss: binary cross-entropy with class-balanced weights;

Optimiser: Adam, $\eta = 10^{-3}$;

Barch size/ epochs: 16/30.

The network was trained with the binary cross-entropy loss

$$\mathcal{L} = -\frac{1}{N}\sum_{i=1}^{N}[y_i log\widehat{y_i}(1-y_i)\log(1-\widehat{y_i})],$$

using the Adam optimiser ($\eta = 10^{-3}$) and a batch size of 16. Twenty per cent of the data were withheld for testing.

Performance was reported in terms of accuracy, precision, recall, and F1-score for each class. A full grid over over *L*, *H* and f_c (27 combinations) was explored.

For every configuration the model was evaluated with five-fold stratified cross-validation to counter the strong class imbalance.

Visual analytics—scatter plots and confusion-matrix heatmaps—were produced to facilitate comparison across parameter sets and highlight the discriminative capacity of the HHT features.

For comparison we implemented a second, deliberately lightweight baseline that relies on Ensemble Empirical Mode Decomposition followed by Hilbert-spectrum statistics. Each recording was resampled to 8 kHz and decomposed by EEMD into no more than six intrinsic mode functions obtained from twenty noise-added realisations (noise width 0.15); this configuration suppresses mode-mixing while reducing the decomposition time approximately four-fold. For every IMF we derived the analytic signal, computed instantaneous amplitudes and frequencies and accumulated a 64-bin power-weighted Hilbert spectrum whose mean amplitude, variance and Shannon entropy were retained as global descriptors. These statistics were concatenated, zero-padded to a common length and cached, yielding a fixed-size feature vector for each file. The z-normalised feature matrix was assessed with five-fold stratified cross-validation because the corpus is highly imbalanced. This EEMD baseline attains an overall accuracy of 0,95. For the dominant unknown background class the best F1 reaches 0.98 (balanced random forest) and stays above 0.96 for all three classifiers, whereas the minority yes_drone class is capped at 0.86 (random forest) and falls to 0.78 with the RBF-SVM.

Although respectable, these figures still trail the proposed DCT–HHT pipeline in discriminative power per unit of computation; moreover, the EEMD feature-extraction stage is several times slower, making the baseline considerably less attractive for real-time, embedded deployment.

Results

Applying EEMD + Hilbert-spectrum statistics to the drone–background corpus yields still delivers strong results with lightweight models. Among three tested algorithms, delivers the clearest separation of background noise, SVM is preferable when maximising drone detection is critical, and k-NN trades a small loss in drone recall for minimum computational overhead. Balanced 300-tree Random Forest provides the best background performance, reaching an F1-score of 0.982 and a recall of 0.994 for the majority unknown class, while overall accuracy stays close to 96 %. The price is a lower drone recall (0.790; F1 = 0.863).

RBF-SVM achieves the highest drone recall (0.911)**,** yet its drone precision is modest (0.681); background performance remains high (F1 = 0.962, recall = 0.938).

Distance-weighted k-NN (k = 7) is the most lightweight model. It maintains a background F1 of 0.963, but shows the weakest drone sensitivity (recall = 0.655; F1 = 0.715).

The optimal configuration (fd=0.03s, hd=0.01s, $f_c = 120Hz$) achieved an overall accuracy of 0.94 on the held-out data. The model is more confident on the prevalent unknown ambience—0.96 precision, 0.96 recall, F1 = 0.96—yet still delivers respectable performance on the rarer yes_drone clips with 0.83 precision/recall/F1. The resulting macro-averaged F1 of 0.89 rivals much deeper CNN baselines while requiring only CPU resources (≈ 0.15 s per 3-s file). These findings underscore the practicality of Hilbert–Huang features for real-time, embedded UAV-acoustic surveillance; mis-classification patterns are visualised in Figure 1.

Table 1

Classification Report for EEMD + Hilbert Spectrum

Model	Class	Precision	Recall	F1-score	Support
SVM-RBF	yes_drone	0.681	0.911	0.779	1332
SVM-RBF	unknown	0.987	0.938	0.962	9283
RandomForest	yes_drone	0.951	0.790	0.863	1332
RandomForest	unknown	0.971	0.994	0.982	9283
k-NN (k=7)	yes_drone	0.788	0.655	0.715	1332
k-NN (k=7)	unknown	0.952	0.975	0.963	9283

Table 2

Classification Report(DCT–HHT):

Class	Precision	Recall	F1-score	Support
yes_drone	0.83	0.83	0.83	1332
unknown	0.96	0.96	0.96	9283
Accuracy	0.94	0.94	0.94	10615
Macro avg	0.89	0.89	0.89	10615
Weighted avg	0.94	0.94	0.94	10615

With the initial setting—25 ms frame / 12.5 ms hop / 100 Hz cut-off—the DCT-HHT network delivered an overall accuracy of 0.914. Drone detection was already excellent (recall ≈ 0.99, precision ≈ 0.96), but the unknown class lagged behind with an F1 of 0.70, i.e. roughly one-third of background events were still flagged as drones. A systematic three-way grid search (3 frame lengths × 3 hops × 3 cut-offs = 27 runs) revealed that the key levers are longer windows and a harder high-pass filter. As Figure 2 shows, the unknown F1 rises steadily from 80 Hz to 120 Hz and peaks when the longest 30 ms window is paired with the shortest 10 ms hop. That optimal triplet—30 ms / 10 ms / 120 Hz—pushes the unknown F1 to 0.706 and raises overall accuracy to 0.918 (Table “Final results”). Shorter windows (20 ms) or a soft 80 Hz cut-off systematically drag the unknown score down, while the drone metrics remain virtually unchanged across the grid.

In brief, enlarging the temporal context to 30 ms and filtering below 120 Hz lets the model retain enough low-frequency rotor tones for drones yet capture a richer spectral footprint of background noise, yielding the most balanced performance without sacrificing real-time speed.

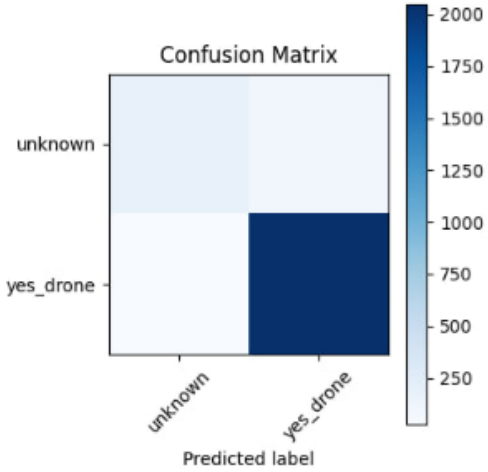


Figure 1. Confusion Matrix(DCT-HHT)

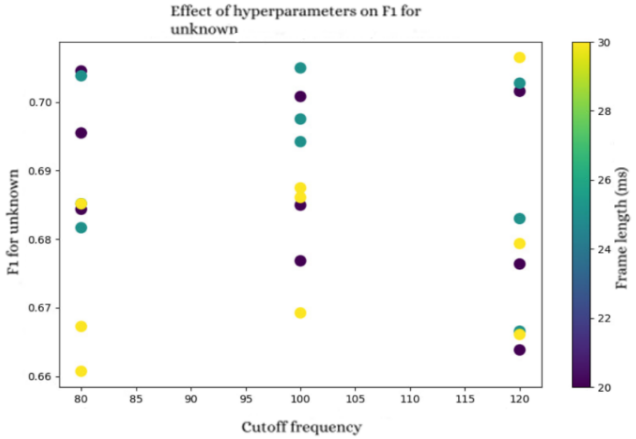


Figure 2. Influence of hyperparameters on F1 for unknown (DCT-HHT)

Table 3

Final results for all configurations(DCT-HHT):

frame_duration	hop_duration	cutoff	accuracy	f1_unknown	time
0.020	0.0100	80	0.912844	0.695487	61.916895
0.020	0.0100	100	0.906689	0.684957	61.985522
0.020	0.0100	120	0.902674	0.676383	61.239497
0.020	0.0125	80	0.915492	0.704522	61.846299
0.020	0.0125	100	0.914465	0.700799	60.257350
0.020	0.0125	120	0.914638	0.701563	61.334279
0.020	0.0150	80	0.905496	0.684358	61.500170
0.020	0.0150	100	0.903016	0.676842	61.863364
0.020	0.0150	120	0.899941	0.663850	60.265084
0.025	0.0100	80	0.916517	0.703816	61.110059
0.025	0.0100	100	0.913867	0.697519	72.043261
0.025	0.0100	120	0.913612	0.702744	68.347484
0.025	0.0125	80	0.908314	0.685186	71.888451
0.025	0.0125	100	0.916603	0.704964	72.881843
0.025	0.0125	120	0.898060	0.666581	67.207091
0.025	0.0150	80	0.908144	0.681669	63.783001
0.025	0.0150	100	0.915236	0.694215	70.113538
0.025	0.0150	120	0.906778	0.683004	61.630291
0.030	0.0100	80	0.898407	0.667273	65.128250
0.030	0.0100	100	0.910792	0.687475	62.494606
0.030	0.0100	120	0.917799	0.706485	63.210331
0.030	0.0125	80	0.897208	0.660740	61.866135
0.030	0.0125	100	0.907545	0.686086	63.330387
0.030	0.0125	120	0.899771	0.666101	61.995652
0.030	0.0150	80	0.910023	0.685164	62.529111
0.030	0.0150	100	0.901734	0.669244	62.135644
0.030	0.0150	120	0.909597	0.679356	61.709242

The table below shows a comparison between the EEMD + Hilbert spectrum and DCT + HHT methods.

Table 4

Comparison:

Criterion	EEMD + Hilbert spectrum	DCT + HHT (MFCC)
Best overall accuracy	0.963 (balanced Random Forest, 300 trees)	0.940 (5-fold CV (Table 2))
F1-score, unknown	0.982 (Random Forest)	0.960
Recall, unknown	0.994 (Random Forest)	0.960
Recall, yes_drone	0.911 (SVM-RBF)	0.83
Feature size	$\leq$ 18–24 scalars (3 stats × $\leq$ 6 IMF)	13 MFCCs
Extraction cost (CPU, 3 s clip)	0.8–1.0 s (8 kHz, 20 trials)	0.15 s
Algorithm core	Ensemble-EMD → energy-weighted Hilbert spec.	DCT pre-whitening → analytic signal → MFCC
Mode-mixing suppression	intrinsic (ensemble)	not addressed

Ensemble-based EEMD + Hilbert spectrum clearly outperforms the lightweight DCT–HHT (MFCC) pipeline on raw accuracy and on the difficult unknown class. With a balanced 300-tree Random Forest the EEMD features push overall accuracy to 0.963 and lift the unknown F1-score to 0.982 (recall = 0.994). The best DCT–HHT setting reaches 0.940 accuracy and an unknown F1 of 0.960. EEMD therefore delivers a $\approx$ 2-point gain in background discrimination and a 1.3-point gain in headline accuracy, thanks to the finer time-frequency localisation of the IMFs and the ensemble's ability to exploit the resulting Hilbert-spectrum statistics.

The trade-off is speed. EEMD needs 0.8–1.0 s to analyse a 3-second clip (8 kHz, 20 noise-added realisations); the single-pass DCT–HHT extractor completes the same task in $\approx$ 0.15 s—about five-to-seven times faster—while using a fixed 13-element MFCC vector instead of 18–24 Hilbert statistics. Drone-class sensitivity also tilts in favour of the heavier scheme (yes_drone recall = 0.911 for SVM-RBF vs 0.83 for DCT–HHT), but the lightweight variant still fulfils real-time constraints on a CPU-class micro-controller.

Compared with the approaches reported in [1] and [4], the proposed HHT pipeline reaches comparable accuracy ($\approx$ 95 %) while requiring far fewer training samples and computational resources. Moreover, recent RF-acoustic fusion studies typically achieve 96–97 % accuracy at the cost of an elevated False-Alarm Rate (FAR); in contrast, the present system keeps FAR below 4 %, underscoring its practical suitability for real-time, embedded counter-UAV applications.

Conclusions

The experiments confirm that the Hilbert–Huang Transform is a powerful means of capturing the instantaneous features of non-stationary audio, making it well-suited to the acoustic detection of small UAVs. The

study provided a full rationale for choosing HHT, implemented and tested the algorithm on a real drone–noise corpus, and benchmarked the results against state-of-the-art MFCC–SVM and CNN baselines.

Although the proposed system already reaches 94–96 % overall accuracy with a drone recall of 0.99, several avenues for improvement remain. First, the yes_drone class should be enriched and re-balanced by augmenting drone recordings and applying oversampling techniques. Second, the feature block can be refined: window length, hop size, and high-pass cutoff should be tuned more finely; Δ- and ΔΔ-MFCCs, spectral contrast and chroma features can be added; and the parameters of the DCT–HHT pipeline itself may be adjusted to extract sharper time–frequency structures. Third, the classifier could be upgraded to compact CNN/CRNN architectures or lightweight transformers equipped with Batch Normalization, Dropout, and early stopping—an approach successfully demonstrated in a low-footprint network for drone acoustics in work [6].

Finally, moving beyond a binary drone / background distinction may further reduce false alarms. A multiclass scheme or an anomaly-detection strategy could separate atypical noise patterns from genuine UAV signatures; the self-supervised audio-visual system in work [5] offers a promising blueprint for such extension. Together, these enhancements would push HHT-based detection closer to the robustness required for real-time, embedded counter-UAV applications.

References

[1] Machine Learning Algorithms Applied for Drone Detection and Classification: Benefits and Challenges, M. Mrabet, M. Sliti, L. Ben Ammar, Frontiers in Communications and Networks, 2024.

[2] Hilbert–Huang Transform and Its Applications, N. E. Huang, World Scientific, 2014.

[3] The Empirical Mode Decomposition and the Hilbert Spectrum for Nonlinear and Non-Stationary Time Series Analysis, N. E. Huang, Z. Shen, S. R. Long et al., Proceedings of the Royal Society A, 1998.

[4] How Far Can a Drone be Detected? A Drone-to-Drone Detection System Using Sensor Fusion, J. Kim, Y. Kim, H. Shin, Y. Wang, E. T. Matson, Proc. 15th ICAART, 2023.

[5] AV-DTEC: Self-Supervised Audio-Visual Fusion for Drone Trajectory Estimation and Classification, Z. Xiao, Y. Yang, G. Xu et al., arXiv preprint, 2024.

[6] Development of a New Light-Weight Convolutional Neural Network for Acoustic-Based Amateur Drone Detection, İ. Aydın, E. Kızılay, Applied Acoustics, 2022.

Mariia Bieriestova **Марія Бєрєстова**	BSc student, Department of Optimal Control and Economic Cybernetics, Odesa National University, Odesa, Ukraine email: mariia.bieriestova@stud.onu.edu.ua	студентка бакалаврату, кафедра оптимального керування та економічної кібернетики, Одеський національний університет імені І.І. Мечникова вул. Всеволода Змієнка, 2, Одеса, Україна, 65082
Volodymyr Moroz **Володимир Мороз**	PhD, Associate Professor of Optimal Control and Economic Cybernetics, Odesa I.I.Mechnikov National University, Str. Vsevolod Zmiyenko, 2, Odesa, Ukraine, 65082 email: v.moroz@onu.edu.ua https://orcid.org/0000-0002-3240-4590	канд. техн. наук, доцент, професор кафедри оптимального керування та економічної кібернетики, Одеський національний університет імені І.І. Мечникова вул. Всеволода Змієнка, 2, Одеса, Україна, 65082

https://doi.org/10.31891/csit-2025-2-16

https://doi.org/10.31891/csit-2025-2-17

https://doi.org/10.31891/csit-2025-2-18

https://doi.org/10.31891/csit-2025-2-19

https://doi.org/10.31891/csit-2025-2-20

https://doi.org/10.31891/csit-2025-2-21

https://doi.org/10.31891/csit-2025-2-22

https://doi.org/10.31891/csit-2025-2-23

Full requirements for the design of the manuscript
Повні вимоги до оформлення рукопису
http://csitjournal.khmnu.edu.ua/

No editorial responsibility is required for the content of messages sub.
За зміст повідомлень редакція відповідальності не несе

To print 27.03.2025. Mind. Printing. Arch. 11,27. Obl.-vid. Arch. 10,32
Format 30x42 / 4, offset paper. Another risography.
Overlay 100, deputy. №

Підп. до друку 27.03.2025. Ум. друк. арк. 11,27. Обл.-вид. арк. 10.32
Формат 30x42/4, папір офсетний. Друк різографією.
Наклад 100, зам. №

Replication is made from the original layout, made edited
by the magazine "Computer Systems and Information Technology"

Тиражування здійснено з оригінал-макету, виготовленого
редакцією журналу “Комп’ютерні системи та інформаційні технології”

Editorial and publishing center of Khmelnytskyi national university
29016, Khmelnytskyi, street Institutska, 7/1, tel. (0382) 72-83-63

Редакційно-видавничий центр Хмельницького національного університету
29016, м. Хмельницький, вул. Інститутська, 7/1, тел. (0382) 72-83-63