МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська політехніка»

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 14, № 1-2

Volume 14, No. 1-2

Одеса – 2024
Odesa – 2024

Журнал внесений до переліку наукових фахових видань України (технічні науки) згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р. Перереєстровано на категорію «Б» за фахами 121, 122, 125, 151 згідно наказу МОН України № 1473 від 26.11.2020 р.

Виходить 4 рази на рік

Заснований Одеським національним політехнічним університетом у 2011 році

Свідоцтво про державну реєстрацію КВ № 17610 - 6460Р від 04.04.2011р.

Published 4 times a year

Founded by Odesa National Polytechnic University in 2011

Certificate of State Registration KB № 17610 - 6460P of 04.04.2011

Друкується за рішенням редакційної колегії та Вченої ради Національного університету «Одеська політехніка»

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: 1, Шевченка пр., Одеса, 65044, Україна
Телефон: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

Editorial address: 1, Shevchenko Ave., Odesa, 65044, Ukraine
Tel.: +38 048 705 8506
Web: www.immm.op.edu.ua (immm.opu.ua) E-mail: immm.ukraine@gmail.com

ЗМІСТ/CONTENTS

DOI 10.15276/imms.v14.no1-2.5
UDC 616-093

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 5-11

DEVELOPMENT OF AN ALGORITHM FOR THE FUNCTIONING OF A SYSTEM FOR REMOTE MONITORING OF THE PSYCHO-PHYSIOLOGICAL STATE OF A PERSON

V.V. Bagriy, R.V. Voloshin, O.O. Zhulkovskyi, K.R. Voloshina

Dniprovsky State Technical University
2, Dniprobudivska str., Kamianske, 51918, Ukraine;
email: olalzh@ukr.net

The issue of maintaining human health is an important area of medicine. Today, there are many diagnostic, therapeutic and preventive measures and technologies aimed at improving the quality of health and increasing the life expectancy of the population. All existing diagnostic techniques are performed in direct contact with the patient and the doctor. At present, there is a rather low level of equipment with various medical and diagnostic devices, as well as a low professional level of medical staff. This has resulted in an increase in morbidity and mortality, and a real decline in life expectancy in Ukraine, which has been observed especially in recent years. Today, medicine is facing the issue of early diagnosis with a high probability of making an accurate diagnosis. This requires the development of methods and technical means of high sensitivity and specificity of equipment for determining biometric indicators and studying the measurement channels of biomedical parameters. The literature review has shown that in order to develop command control systems and speech-to-text conversion in a fused speech stream, it is necessary to use «mechanisms» for automatic recognition and understanding of the operator's speech. However, these «mechanisms» have some shortcomings, due to a large number of interferences. The main goal of the work is to develop a device for diagnostic processing and obtaining biomedical parameters for further analysis and electrophysiological studies, which will generally increase the reliability of diagnostics. The algorithm of operation of the system for remote monitoring of the psycho-physiological state of a person based on heart rate and electrocardiological signal is presented. One of the ways to improve the quality of human health prevention is to improve the quality of diagnostics of the functioning of human organs. It is possible to improve the quality of diagnostics by early detection of deviations from the norm of their functioning. It is known that the use of so-called «smart» clothing is gaining popularity. When testing and creating algorithms for processing experimentally obtained signals, it is necessary to thoroughly check them to assess the reliability of recognising informative fragments, the accuracy of measuring diagnostic features focused on these fragments, as well as a number of other indicators.
Keywords: system algorithm, heart rate, electrophysiological methods, electrocardiogram, microprocessor unit, microcontroller, remote monitoring.

Introduction. The problem of maintaining human health is an important aspect of medical science. Nowadays, there are many methods of diagnosis, treatment and prevention aimed at improving health and increasing the life expectancy of the population. All of these methods are usually performed during direct contact between the patient and medical staff. However, today we can observe an insufficient level of medical equipment in various healthcare facilities, as well as an insufficiently high professional level of medical staff. This leads to an increase in morbidity and mortality among the population, which leads to a real decrease in life expectancy in Ukraine, especially noticeable in recent years.

One of the main challenges in medicine is the need for timely diagnostics with high accuracy. This requires the development of highly sensitive and specific methods and technical means for determining biometric parameters and studying medical indicators.

Literature review. Today, so-called «smart» clothing (wearable technology), which can be used to monitor health indicators, is becoming increasingly popular. «Smart» clothing is clothing that can interact with the environment by sensing signals, processing information and

triggering responses. In «smart» clothing, fabric electrodes are actively used to capture the electrocardiogram signal [1, 2]. However, the signal obtained using such electrodes has a significant drawback – a large number of artefacts (noise, various interferences) of various nature. When creating algorithms for processing experimentally obtained signals, they need to be thoroughly tested to assess the reliability of recognising informative fragments, the accuracy of measuring diagnostic features focused on these fragments, as well as a number of other indicators. In addition, in real life, the shape of informative fragments is distorted by various internal and external disturbances, which can only be reduced to additive obstacles in some cases. All this complicates digital signal processing, stimulating the creation of new processing algorithms. In this work, the research vector is aimed at improving the reliability of the diagnosis, using modern advances in microelectronics and nanotechnology [1].

The review and analysis of relevant literature and patent sources on the topic showed that the most valuable information for functional diagnostics is electrophysiological methods based on measuring the bioelectrical activity of various human organs and tissues, in particular the cardiovascular system. These methods are well-known and widely used in practice. However, they have fundamental disadvantages caused by their metrological characteristics.

Research Objective. The main goal of the work is to develop a device for diagnostic processing and obtaining biomedical parameters for further analysis and electrophysiological studies, which will generally increase the reliability of diagnostics. The algorithm of operation of the system for remote monitoring of the psycho-physiological state of a person based on heart rate and electrocardiological signal is presented. One of the ways to improve the quality of prevention of diseases is to improve the quality of diagnostics of organ functioning. Improving the quality of diagnostics is possible through the early detection of abnormalities in their functioning.

Main Body. The algorithm of operation of the device for remote monitoring of the psycho-physiological state of a person is shown in Fig. 1. The algorithm works as follows.

The patient puts on the suspension 2 with the belt part, which should fit the torso and provide «dry» galvanic contact with the nipple areas, one of which is the paracardial area of the anterior chest surface. After the suspension is installed, switch on the power supply (p. 2) by simultaneously pressing the buttons on the monitor unit body.

The next step is to check the functionality of the modules: ADC 12, accelerometer 18, Bluetooth contactless modem 17, RAM 15, clock 19, as well as the creation of a performance table (p. 3). Then the initialization is performed: ADC 12 (sampling rate Fd=500 Hz), accelerometer 18, Bluetooth contactless modem 17, RAM 15, clock 19 (p. 4).

Next, the portable monitor is switched to the monitoring mode (p. 5). At the same time, the ADC is polled (p. 6). Sampling and searching for RR intervals are accumulated in the memory of the microcontroller 13 (p. 7). If the RR interval is found (p. 8), the accelerometer 18 is polled: «Is there a patient movement?» (p. 9). If movement is detected, its duration is determined (p. 24), and if the movement lasts more than 2 seconds, the device is switched to the «sleep» mode (p. 25). During the «sleep» mode, the accelerometer 18 is periodically polled to detect the lack of motor activity in the patient.

If there is no movement for 10 seconds, the device enters the operating mode. When the patient is calm (accelerometer 18 does not show movement, i.e., there are no motion artefacts), the patient's condition is searched for cardiological pathologies (p. 10). To do this, the measured parameters are compared with the parameters obtained in p. 21 during training and the set thresholds:

– heart rate (HR) >140 – paroxysmal tachycardia;
– HR>240 – atrial flutter;
– absence of R-peak;
– arrhythmia (A variable arrhythmia ≥ A reference arrhythmia value + threshold);

– rhythm disturbance (HR number of measurements ≠ HR number of reference measurements, or if: N imperial measurements ≥ N imperial reference measurements with HR number of measurements = HR number of reference measurements);

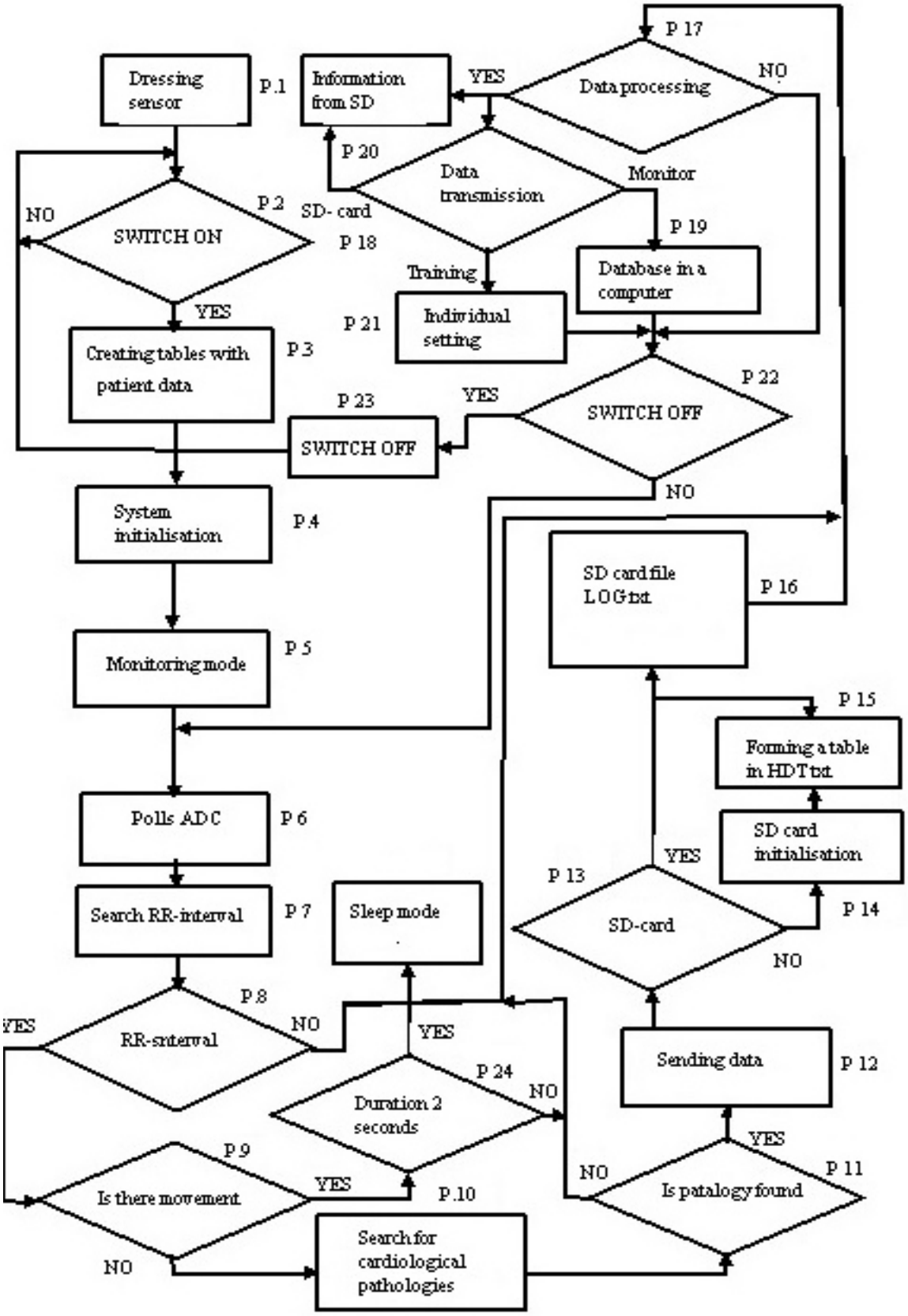


Fig. 1. Algorithm of the remote monitoring system of human psycho-physiological state

– check whether the sign of the P-peak has changed or the sign of the T-peak has changed.

If a pathology is found at the end of the analysis stage (p. 11), the modem 17 communicates with the GSM modem of the patient's phone – the microprocessor generates and sends an SMS message (p. 12).

This message may contain one of the following cardiological diagnoses:

– paroxysmal tachycardia;
– atrial flutter;
– absence of R-peak;
– arrhythmia
– heart rhythm disturbance;
– cardiac arrest;
–prognosis of dangerous ventricular arrhythmias;
– extrasystole;
–dangerous rise of the ST-segment;
– absence of R-peak or negative R-peak;
–absence of T-peak or negative T-peak.

Next, the SD memory card is initialised (p. 13, 14). The performance table (in the form of the HDT.txt file) is saved to it. Then, the LOG.txt file is created on the SD card and a 60-second «fragment» of the signal is saved in the ECG.txt file (p. 16). It is checked whether an external computer is connected via the USB port (p. 17), if so, the microprocessor reads a command from the computer via the USB port (p. 18). Depending on the command, either direct data transfer to the computer is performed (p. 19), or data is read from the SD memory card (p. 20), or the system is individually set up for the patient («training», p. 21).

Next, it checks whether the system needs to be switched off (by simultaneously pressing two buttons on the monitor unit case, p. 22). If «NO», the algorithm returns to p. 7. If «YES», the algorithm returns to p. 2. The algorithm can be run for many days according to this cycle of steps (p. 1-25). If necessary, the device can be switched off by pressing two buttons simultaneously on the monitor unit body (p. 22). Switching the monitor on and off is signalled by a tactile vibration alarm 21, which is mounted on the monitor body and is felt by the patient through the waist part of the bodice. The original design of the spherical electrode matrixes does not have an irritating action on the patient's body and allows for the acquisition of an electrocardiological signal (ECG), a signal with sufficient reliability for emergency diagnosis [4, 5].

The main advantage of the device is the ability to use ECG shapes in patients with pathology, which is ensured by the individual patient adjustment mode. In addition, the device allows to differentiate ECG signals obtained during patient movement from signals of cardiac emergencies due to the elimination of motion artefacts. In the presence of intense patient movements, the device's power supply is switched to sleep mode, which significantly extends the monitor's life [4, 5].

A mobile monitor for a cardiology patient, an electrocardiogram (ECG) block containing an analogue-to-digital converter (ADC), a removable memory card, connected to a microcontroller. The latter is distinguished by the fact that it additionally includes means for generating SMS messages through a GSM telephone modem, a three-axis accelerometer, a real-time clock, a USB port for communication with external devices, a common-mode interference suppression unit associated with a microcontroller and an operational device (RAM). At the same time, the ECG block contains two electrode arrays made with the possibility of fixing and «dry» contact with the areas of the front surface of the chest. Each matrix contains two groups of electrodes, one of which is connected to the in-phase interference suppression unit, and the other to the inputs of the operational amplifier, the output of which is connected to the ADC through a filter. At the same time, the microcontroller is designed to store individual ECG parameters of the patient in the RAM and compare them with the ECG parameters of the current monitoring, taking into account the ECG parameters, according to the established criteria. The ECG parameters are obtained in

the absence of motion artifacts recorded by the 3-axis accelerometer, and if the ECG parameters of the current monitoring differ from the individual ECG parameters of the patient by more than the critical value, an SMS with a diagnosis is generated via the GSM modem of the phone.

As shown in Fig. 1, the algorithm can be seen that in the presence of motion artefacts registered by the 3-axis accelerometer, the microcontroller goes into sleep mode (p. 25) and the ECG unit is turned off (p. 22).

When changing memory cards, ECG parameters are entered into the table, or an SMS message with ECG parameters is transmitted (if a smartphone is used for data transmission) from the moment the parameters are formed in p. 19. Note that p. 8 distinguishes which ECG parameters determine the preferred duration of RR intervals, time and amplitude characteristics of the QRS complex and ST segment.

P. 1, is responsible for the installation of a bodice-type suspension on the patient, with the electrode matrices of the ECG block placed in the waist part of the bodice, connected by flexible wires to the device body, on the walls of which are mounted a three-coordinate accelerometer, a tactile vibration alarm and power buttons. The body itself is designed to fit into a pocket of a person's waistband.

With the development of telemedicine, an acute problem has arisen in the manufacture of tonometers that can be wirelessly connected to a PC or smartphone using a Bluetooth channel or other suitable modem. The stages of using such devices are as follows [6]:

– data transfer to a PC or smartphone;
– collection of statistics, the ability to analyse the collected data;
– derivation of trends.

The smartphone is used not only for data collection, but also for control with the ability to view pulse wave graphs.

Each block and its purpose is described in more detail below. Fig. 2 shows the functional electrical circuit of the complex for wireless remote monitoring of the human psycho-physiological state [1-5].

The developed device can be divided into several functional blocks:

– signal registration
– analogue processing;
– microprocessor block;
– power supply unit;
– visual presentation of results;
– data transmission block.

Conclusions. The work provides an analytical review of scientific and technical publications and patents on medical technology and biometric engineering in the field of monitoring the physiological state of the human body with a view to further developing technical means for assessing pathological changes in the human condition. The ways of building relevant devices using wireless networks are planned.

The algorithm of operation of the system for remote monitoring of the psycho-physiological state of a person using tissue electrodes is developed, and the functional diagram of the complex for wireless remote monitoring of the psycho-physiological state of a person is presented.

The results of this study can be used to create a system for monitoring a person's condition based on their ECG.

The results of the study point to new directions for improving the electrocardiograph's work.

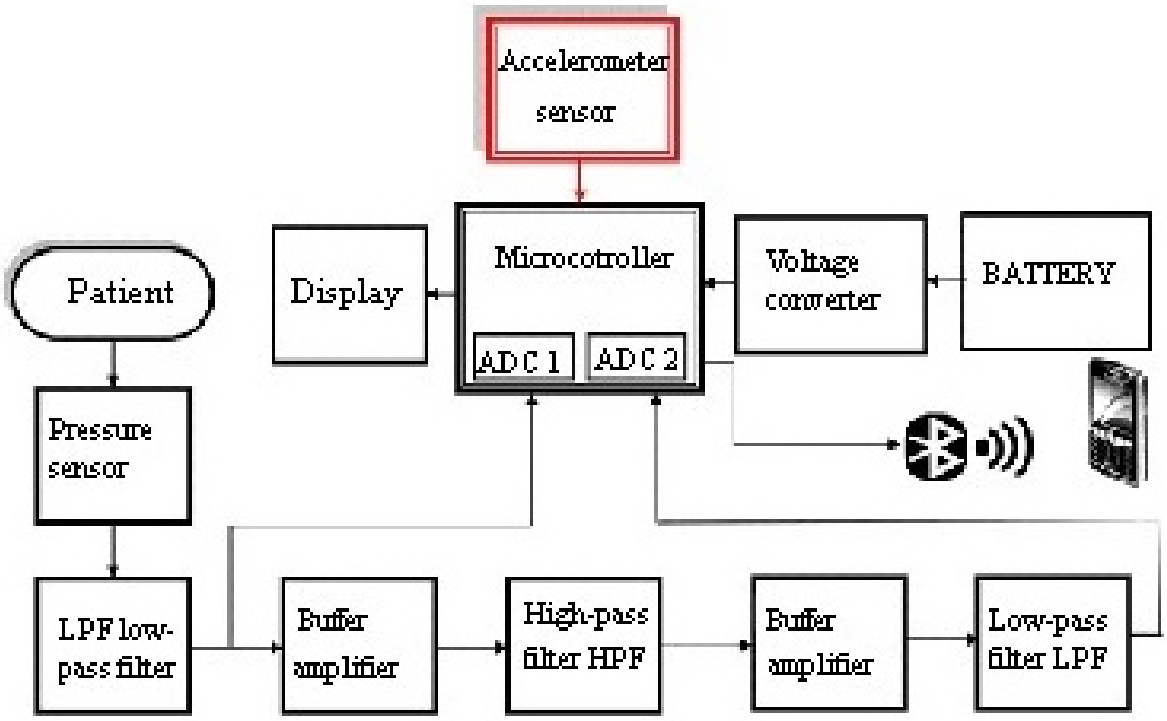


Fig. 2. Functional electrical circuit of the complex for wireless remote monitoring of human psycho-physiological state [6]

References

1. Kornatskyi V.M. Problemy zdorovia suspilstva ta prodovzhennia zhyttia. Kyiv: Instytut kardiolohii im. M.D. Strazheska, 2006. 46 s.
2. Vorobev L.V. Analyz ECG zdorovoho cheloveka. Kremenchuh: 2017. 102 c.
3. Kypenskyi A.V., Shamardyna V.N., Deineko D.M. Elektrokardyohrafyia. Kharkov: NTU «KhPY», 2002. 52 s.
4. Bagriy V., Trikilo A., Gulesha O., Voloshin R. Mathematical modeling and analysis of human cardiovascular system indicators. *Математичне моделювання*. 2022. №1 (46). С. 141-147. URL: https://doi.org/10.31319/2519-8106.1(46)2022.258458
5. Bahrii V.V., Trykilo A.I., Voloshyn R.V. Mikroprotsesornyi prylad dlia otrymannia bioelektrychnoi informatsii. *Zbirnyk naukovykh prats Dniprovskoho derzhavnoho tekhnichnoho universytetu (tekhnichni nauky)*. 2023. №1 (42). S. 109-119. URL: https://doi.org/10.31319/2519-2884.42.2023.13
6. Meshchanynov S.K., Trykylo A.Y., Voloshyn R.V. Adaptyvno-synerhetycheskaia model systemy otsenky sostoianyia zdorovia cheloveka. *Zbirnyk naukovykh prats Dniprovskoho derzhavnoho tekhnichnoho universytetu (tekhnichni nauky)*. 2013. №1 (21). S. 131-137.
7. Chaudhari M., Dharavath S. Study of Smart Sensors and their Applications. International *Journal of Advanced Research in Computer and Communication Engineering*. 2014. Vol. 3, №1.
8. Shriufer E. Obrobka syhnaliv. Tsyfrova obrobka dyskretyzovanykh syhnaliv. K: Lybid, 1992. 294 s.
9. Boiko V.I. Stokhastyka elektronnykh system. K., 2007. 380 s.
10. Gupta V. A Study of Various Face Detection Methods. *International Journal of Advanced Research in Computer and Communication Engineering*. 2014. Vol. 3, №5. p. 6694-6697.

РОЗРОБКА АЛГОРИТМУ ФУНКЦІОНУВАННЯ СИСТЕМИ ДИСТАНЦІЙНОГО МОНИТОРИНГУ ПСИХОФІЗІОЛОГІЧНОГО СТАНУ ЛЮДИНИ

В.В. Багрій, Р.В. Волошин, О.О. Жульковський, К.Р. Волошина

Дніпровський державний технічний університет
2, Дніпробудівська вул., Кам'янське, 51918, Україна
email: olalzh@ukr.net

Проблема збереження здоров'я людини є важливим напрямом медицини. Нині існує безліч діагностичних, лікувальних і профілактичних заходів та технологій, спрямованих на підвищення якості здоров'я, збільшення тривалості життя населення. Усі існуючі діагностичні методики виконуються при безпосередньому контакті хворого з лікарем. Наразі спостерігається достатньо низький рівень оснащеності різної лікувальної та діагностичною апаратурою, так само як і низький професійний рівень лікарського складу. Наслідком цього є зростання захворюваності і смертності населення, реальне зниження тривалості життя населення України, що відмічається особливо останніми роками. Зараз у медицині стоїть питання ранньої діагностики з високою ймовірністю поставлення точного діагнозу. Це вимагає розробки методів і технічних засобів високої чутливості і специфічності апаратури для визначення біометричних показників та дослідження вимірювальних каналів біомедичних параметрів. Літературний огляд показав що для розробки систем командного керування й перетворення «мова – текст» у потоці злитої мови, необхідно використовувати «механізми» автоматичного розпізнавання та розуміння мови оператора. Але ці «механізми» мають де які недоліки, це пов'язано з великою кількістю завад. Основною метою роботи є розробка пристрою діагностичної обробки, та отримання за його допомогою біомедичних параметрів для подальшого аналізу та електрофізіологічних досліджень, що в цілому підвищить достовірність діагностики. Представлено алгоритм роботи системи дистанційного моніторингу психофізіологічного стану людини за показаннями частоти серцевих скорочень та електрокардіологічного сигналу. Одним із способів підвищення якості профілактики здоров'я людини є поліпшення якості діагностики функціонування її органів. Підвищити якість діагностики можливо шляхом раннього виявлення відхилень від норми їх функціонування. Відомо, що нині набирає популярність використання так званого «розумного» одягу. При тестуванні і створенні алгоритмів обробки експериментально отриманих сигналів потрібна їх ретельна перевірка для оцінки достовірності розпізнавання інформативних фрагментів, точності виміру діагностичних ознак, зосереджених на цих фрагментах, а також ряду інших показників.

Ключові слова: алгоритм системи, частота серцевих скорочень, електрофізіологічні методи, електрокардіограма, мікропроцесорний блок, мікроконтролер, дистанційній моніторинг.

DOI 10.15276/imms.v14.no1-2.12
УДК 004.04

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 12-23

HYBRID ASYMMETRIC CODE-BASED CRYPTOSYSTEM

A.Ya. Davletova

West Ukrainian National University,
11, Lvivska Str. Ternopil, 46009, Ukraine
email: a7davletova@gmail.com

This work addresses the pressing issue of ensuring reliable information protection amidst increasing data volumes and rising numbers of cyber threats. Traditional cryptographic systems, while generally reliable, may prove vulnerable to new types of attacks, especially quantum ones. This highlights the need for exploring and researching more resilient encryption methods. The work proposes a hybrid cryptosystem that combines the McEliece system with the RSA encryption algorithm. This approach leverages the advantages of both methods: the high security level of RSA, based on the difficulty of factoring large numbers, and the resilience of McEliece to quantum attacks due to the complexity of decoding arbitrary linear codes. A distinctive feature of the proposed hybrid system is the use of Galois fields *GF(p)* for all operations, which provides an additional layer of protection and flexibility compared to traditional systems based on binary numeral systems. The integration of two asymmetric cryptographic algorithms, whose resilience is based on solving different mathematical problems, enhances the reliability and security of the proposed system. The use of a common parameter *n* for key generation also simplifies key management and expands the key space by a factor of *n*. This solution combines error protection with cryptographic security, making it a powerful tool for data protection in environments with potentially unreliable communication channels. The research conducted as part of this work focuses on analyzing the effectiveness and security of the proposed hybrid cryptosystem. Special attention is given to characteristics such as relative information transmission speed, ciphertext length, key size, and resistance to cryptanalysis. The results demonstrate the advantages of the hybrid system compared to using each algorithm individually. The findings could form the basis for further development of cryptographic methods for information protection in the face of modern threats.
Keywords: McEliece cryptosystem, RSA encryption algorithm, finite fields of Galois, hybrid cryptosystem, resistance to cryptanalysis.

Introduction. The modern world is increasingly reliant on robust information protection methods that ensure data confidentiality, integrity, and authenticity. With the development of digital technologies and the increase in data volumes transmitted through open communication channels, there is a need to improve existing cryptographic systems. One promising direction in cryptography that can provide the necessary level of security with enhanced efficiency is hybrid systems that combine the advantages of different encryption algorithms.

Traditional cryptographic systems can be vulnerable to new types of attacks, necessitating the development of more resilient encryption methods. Furthermore, many existing encryption algorithms are considered vulnerable to quantum computers. Therefore, researching and developing cryptographic methods that are resistant to both classical and quantum cryptanalysis is a pressing task. The solution to this problem is possible through the integration of the McEliece code-based cryptosystem and the asymmetric RSA encryption algorithm, which allows for the creation of more robust, flexible, and efficient cryptographic solutions that meet modern information protection requirements.

In particular, the combination of RSA and the McEliece cryptosystem using Galois fields *GF(p)* and arithmetic operations in these fields is a promising approach that allows the advantages of both methods to be combined, enhancing encryption efficiency and resilience. McEliece, due to its resistance to quantum attacks, and RSA, based on the complexity of factoring large numbers, form the basis for an effective hybrid cryptosystem.

Analysis of research and publications. Compliance with data protection standards requires the implementation of the most advanced encryption methods, driving the research and adoption of new cryptographic techniques. The use of open communication channels for transmitting confidential information, storing data in digital environments, the increase in cyber-attacks, and information misuse create additional requirements for data security. Hybrid cryptosystems, which combine the robustness and efficiency of various encryption algorithms, can offer optimal solutions for enhancing security and efficiency under these conditions.

The security of most widely used cryptosystems is based on the difficulty of solving specific mathematical problems, such as the factorization of large numbers, discrete logarithms, the use of cryptographic hash functions, lattice-based methods, and others [1-4]. Code-based cryptosystems have limited practical application due to implementation complexity and key sizes. However, given the capabilities of quantum computers, particularly their computational speed, these cryptosystems represent a promising and rapidly developing field [5-8].

The potential applications and development of hybrid cryptographic systems are one of the important areas of research [9-11]. Traditional encryption methods, although quite reliable, can become vulnerable to new types of attacks. Hybrid cryptosystems provide greater resilience and information security by leveraging the strengths of traditional methods while compensating for their weaknesses. This underscores the necessity of exploring and researching alternative and hybrid cryptographic systems.

One of the most studied cryptographic systems is the McEliece scheme, based on error-correcting codes [12-17]. It is known for its ability to control and correct errors in the channel and its resistance to attacks. The system is based on an encryption method that uses matrix multiplication to create keys. The main idea is to use linear codes for encryption, where the generating matrix of the code G is multiplied with random matrices S and P, which form the secret key G', to create the public key. This approach ensures data security based on the properties of linear codes and the complexity of recovering the secret key. Decoding requires the use of complex algorithms, the complexity of which grows exponentially with the key size. This problem is considered NP-complete, as there is no efficient algorithm that can find a solution in polynomial time. This makes McEliece resistant to many classical cryptanalysis methods, including potential attacks using quantum computers.

An analysis of the sources allows us to conclude that the search for new data protection methods in the context of post-quantum cryptography, which is based on new mathematical constructions such as code superpositions, is becoming a relevant alternative for future information security.

Typically, hybrid cryptosystems combine the efficiency of symmetric encryption with the security of asymmetric encryption [18-20]. These systems use the best characteristics of both methods to protect data exchange over potentially insecure channels. Combining two encryption approaches, based on different mathematical problems and methods, will provide a higher level of security. Specifically, McEliece uses encoding based on linear codes, while RSA employs asymmetric encryption based on the difficulty of factoring large numbers into primes. The security of RSA may be threatened by the development of quantum computers, whereas McEliece is considered a post-quantum system. The complexity of decrypting both cryptographic systems grows exponentially relative to the key length, which is considered an NP-hard problem.

The combination of the McEliece cryptosystem and the RSA encryption algorithm demonstrates significant potential for ensuring a high level of security in modern cyber threat conditions, as each of these algorithms has its unique advantages: McEliece's resistance to quantum computing and RSA's resistance to classical attacks. The use of characteristics and operations in the Galois field $GF(p)$ further enhances the efficiency and security of the hybrid system. This approach will provide an additional level of cryptographic protection for use in

information security systems and represents a promising direction for research.

The aim of this work is to enhance the reliability of data encryption systems by integrating algorithms whose robustness is based on solving different mathematical problems.

Hybrid Asymmetric Cryptosystem. The proposed hybrid asymmetric cryptosystem is based on the principles of data encoding according to the McEliece scheme using the algebraic structures of Galois fields *GF(p)* and the RSA encryption algorithm. The modified McEliece cryptosystem in *GF(p)* includes the following steps [12]:

1. Key Generation. Selection of the Generating Matrix G. The dimension of G corresponds to the length of the codeword $r \times n$, where $n = k + r$, k is the number of information symbols, and r is the number of check symbols. An $n \times n$ permutation matrix P is used to reorder the symbols in the codeword. A $k \times k$ secret matrix S is chosen from the elements of *GF(p)* and is used for additional mixing of the message symbols before encoding them. The public key G' is computed as follows:

$$G' = SGP.$$

2. Encoding the original message m by transforming it into the codeword x using the public key matrix G':

$$x = mG'.$$

3. Message Transmission. To provide additional protection, an error vector e can be added to the resulting codeword x. In this case, it can be considered an additional one-time secret key. The weight of the error may exceed the boundaries of *GF(p)* since arithmetic operations performed during decryption include normalizing values to the limits of *GF(p)*. However, it will determine the complexity of decoding the corrupted codeword x'. The error correction process uses the principles of the McEliece system, based on the Hamming error-correcting code.

4. Decryption. Upon receiving the codeword x', which contains an error, the private keys P' and S', which are the inverses of the matrices P and S respectively, are used for decoding, where S' is computed in the Galois field *GF(p)*.

$$S' = S^{-1} \, mod \, (p).$$

Restoration of the original message

$$m = x' \, P' \, S'.$$

Using the Galois Field *GF(p)* in the McEliece scheme offers several advantages compared to traditional implementations in binary numeral systems. Operations in *GF(p)* require fewer computational resources compared to operations on binary strings in a binary system, which is crucial in cryptographic applications where computational efficiency can be critical, especially for large message lengths. Using *GF(p)* allows for a larger key size without compromising resistance to attacks, thereby increasing the amount of information that can be transmitted using the McEliece cryptosystem while maintaining the same level of security.

The RSA encryption algorithm includes the following steps [1]:

1. Key Generation. Select two large random prime numbers, p and q. Compute the modulus n as the product of p and q:

$$n = p \cdot q.$$

Computing the Euler's Totient Function $\varphi(n) = (p-1)(q-1)$.

Choosing the public exponent e, which is an integer satisfying the condition $1 < e < \varphi(n)$ and is coprime with $\varphi(n)$.

Calculating the private exponent d as the multiplicative inverse of e modulo $\varphi(n)$:

$$d \cdot e \equiv 1\big(mod \, \varphi(n)\big).$$

2. Encrypting the message m involves computing the ciphertext. c:

$$c = m^e \, mod(n).$$

3. Decrypting c involves computing m:

$$m = c^d \, mod(n).$$

The RSA algorithm allows for secure encryption and decryption of messages using the public *(e, n)* and private *(d, n)* keys.

The integration of the modified McEliece cryptosystem, based on linear codes in the Galois Field *GF(p)*, and the RSA encryption algorithm is realized by using one of the RSA modules *p*, *q*, or their product *n* as the size of the field. Using *n* as the maximum value for the Galois Field parameter in McEliece means that the matrix *S* can include elements that are components of *GF(n)*, thereby increasing the complexity of encoding. This significantly expands the dictionary from 0 to *n*-1, representing the set of possible keys or matrices used for message encoding and decoding. It also allows for the use of more values to represent data in constructing more complex and resistant cryptographic systems.

The algorithm of the proposed hybrid asymmetric cryptosystem based on codes is provided in the figure. 1.

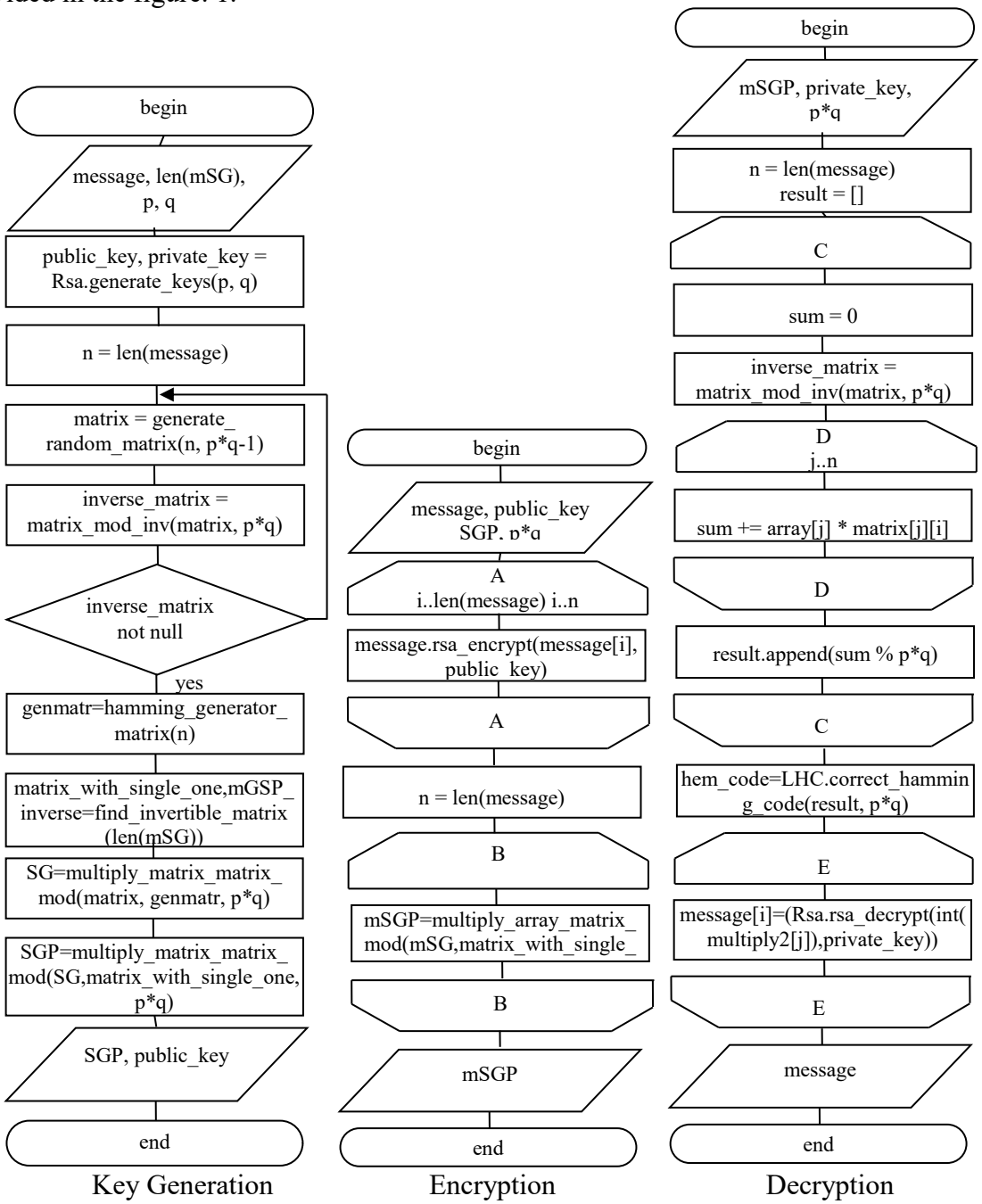


Fig. 1. The algorithm of operation of the hybrid cryptosystem.

For demonstration of the algorithm provided, let's consider an example. Let the plaintext message:

$$m = 9, 5, 11, 28.$$

1. Encryption using RSA:

p=7; q=13; n=91; $\phi(n)$=72; e=5; d=29.

The encrypted message:

$$m' = 81, 31, 72, 84.$$

2. McEliece Encoding. Private Key Generation:

$$G = \begin{matrix} 1110000 \\ 1001100 \\ 0101010 \\ 1101001 \end{matrix} \qquad S = \begin{matrix} 15\ 3\ 35\ 71 \\ 82\ 56\ 18\ 12 \\ 82\ 36\ 40\ 82 \\ 24\ 11\ 9\ 9 \end{matrix} \qquad P = \begin{matrix} 0010000 \\ 1000000 \\ 0000010 \\ 0100000 \\ 0001000 \\ 0000001 \\ 0000100 \end{matrix}$$

Public Key:

$$G' = \begin{matrix} 30\ 18\ 89\ 3\ 71\ 15\ 35 \\ 21\ 86\ 59\ 56\ 12\ 82\ 18 \\ 22\ 67\ 18\ 36\ 82\ 82\ 40 \\ 42\ 29\ 44\ 11\ 9\ 24\ 9 \end{matrix}$$

As a result of encoding, we obtain the message

$$x = 3, 9, 16, 35, 43, 29, 22.$$

Adding an error vector

$$e = 0\ 0\ 21\ 0\ 0\ 0\ 0.$$

We obtain a message corrupted by errors

$$x' = 3, 9, 37, 35, 43, 29, 22.$$

3. Decoding. Computing the inverse matrices S and P:

$$S' = \begin{matrix} 58\ 82\ 53\ 22 \\ 1\ \ 6\ 26\ \ 0 \\ 76\ 49\ 87\ 49 \\ 31\ 89\ 23\ 34 \end{matrix} \qquad P' = \begin{matrix} 0100000 \\ 0001000 \\ 1000000 \\ 0000100 \\ 0000001 \\ 0010000 \\ 0000010 \end{matrix}$$

Restoring the order of symbols in the message x′ P' = 37, 3, 29, 9, 35, 22, 43

Determining error position by recalculating and comparing parity symbols:

p1	16	37
p2	3	3
p3	9	9

As a result, we obtain the binary error position value 100, which corresponds to position 1. In this case, no correction is needed since this position contains a parity symbol.

Information symbols: $m'S'$ = 81, 31, 72, 84.

4. RSA Decryption: m = 9, 5, 11, 28.

The proposed hybrid asymmetric cryptosystem provides additional protection and complexity against cryptanalysis. Combining systems based on different mathematical principles, notably McEliece utilizing coding theory in the Galois field *GF(p)*, where operations are performed on field elements, while RSA employs modular arithmetic operations with large prime numbers, complicates cryptanalytic attacks and ensures a high level of security.

McEliece and RSA serve different application scenarios. McEliece is known for its resistance to lattice-based attacks and quantum computers, whereas RSA is efficient for encrypting short messages and digital signatures. Combining these two methods preserves McEliece's resilience while leveraging RSA's efficiency for rapid encryption of short messages.

The ability to choose the field size provides flexibility in configuring cryptographic

parameters, as the values of p and q depend on specific security and system efficiency requirements. This enables achieving optimal efficiency in cryptographic applications.

Research of the Proposed Cryptosystem. Comparing the efficiency of cryptosystems, we will use criteria such as relative transmission speed, ciphertext length, key size, and resistance to cryptanalysis for each variant.

Relative transmission speed - the ratio of useful information volume to the total volume of transmitted data per unit of time, including all overheads associated with cryptography [21].

For the McEliece scheme, which uses Hamming codes to ensure cryptographic security, the plaintext size is k bits, and the ciphertext size is x, where $x > k$. Efficiency is determined as follows:

$$E_{\text{McEliece}} = \frac{k}{x}.$$

This indicator characterizes the degree of utilization of error-correcting code information capabilities in sequences of length n. For the McEliece cryptosystem in the Galois field $GF(p)$, $E_{McEliece\_}$ is defined similarly as the ratio of information quantity k to the length of the codeword x.

For the RSA algorithm, the relative data transmission speed is determined by the ratio between the key size n and the size of the original message k bits. A larger key size allows for encrypting or decrypting more information simultaneously

$$E_{RSA} = \frac{k}{n}.$$

The size of the plaintext k is limited by the modulus size n, i.e., $k < n$, and the encrypted message x will be almost equal to the size of the modulus n. Therefore, the data transmission efficiency approaches 1.

Table 1 presents the results of conducted research reflecting the relative data transmission speed E at different values of plaintext k and encrypted message x.

Table 1

Relative Data Transmission Speed

k	x	$E_{McEliece}$	E_{Hybrid}
4	7	0,571429	0,571429
11	15	0,733333	0,733333
26	31	0,83871	0,83871
57	63	0,904762	0,904762
120	127	0,944882	0,944882
247	255	0,968627	0,968627
502	511	0,982387	0,982387
1013	1023	0,990225	0,990225
2036	2047	0,994626	0,994626
4083	4095	0,99707	0,99707
8178	8191	0,998413	0,998413

The relative transmission speed allows you to understand which part of the key is used for information processing, and which part is used for additional operations to ensure the security and reliability of the cryptographic process. From the data in Table 1, it can be seen that $E_{McEliece}$ and E_{Hybrid} are inferior to E_{RSA} due to the redundancy associated with the use of error correction codes. However, as the size of the plaintext k increases, the efficiency can increase, since the control characters occupy a relatively smaller share of the total volume of transmitted data.

Figure 2 illustrates the data obtained as a result of studies of the relative speed of data transmission at different lengths of input and output messages for different encryption

algorithms, while for McEliece and hybrid systems, the condition was taken into account $2^r \leq k + r + 1$.

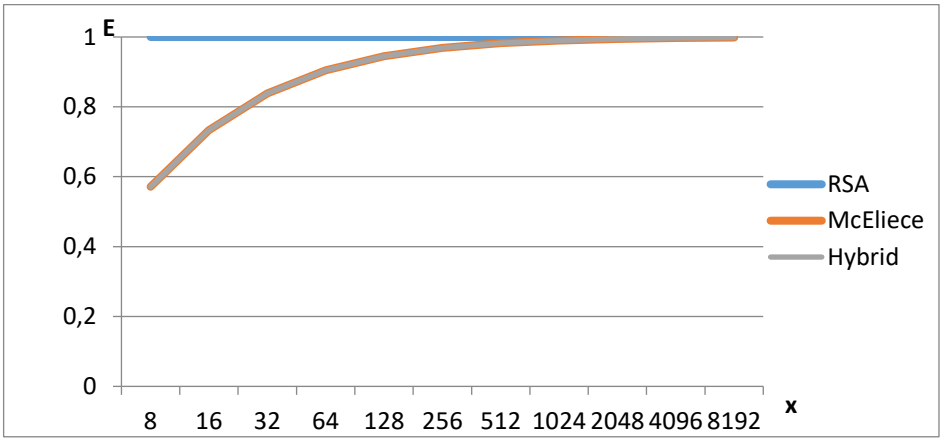


Fig. 2. Change in the relative speed of information transfer when the size of the message changes.

From the obtained data, it is evident that both for the McEliece system and the hybrid system, the relative data transmission speed increases with the size of the message. This means that the larger the amount of data to be transmitted, the closer the efficiency approaches 1, which is a desirable property of a cryptographic system.

The key size is a critical parameter that affects cryptographic strength, computational speed, memory usage, bandwidth, energy consumption, and key storage security. Balancing these aspects is important when choosing the optimal key size for a specific application. Key parameters in McEliece depend on the parameters of the code used, such as the number of rows r and the number of columns k of the generator matrix G', as well as the size of the elements in this matrix.

$$L_{McEliece} = r \times k \times log_2(n),$$

where n is the size of the field in which the elements of the matrix G' are defined, in particular for classical McEliece n=2 for binary fields.

The size of an RSA key is typically determined by the length of the modulus n in bits, which is obtained by multiplying two prime numbers p and q:

$$L_{RSA} = log_2(p \times q).$$

In Table 2, data is provided demonstrating the size of key data L for transmitting data m = 4 symbols at various field sizes n.

Table 2

Size of keys

n	$L_{McElice}$	L_{RSA}	L_{Hybrid}
35	28	6	174
221	28	8	232
899	28	10	290
1517	28	11	319
7387	28	13	377
10403	28	14	406
145157	28	18	522
826277	28	20	580

The analysis showed that the size of the McEliece key does not depend on the value of n, it remains constant at 28 bits. The size of RSA key data increases with n to ensure necessary cryptographic strength. The hybrid system combines elements of McEliece and RSA, explaining the increase in key size. This indicates that the system adapts to changes in

n, providing corresponding cryptographic resilience.

Figure 3 shows graphs depicting changes in the key size of the cryptographic system for encrypting the output message *m*=4 depending on *n*.

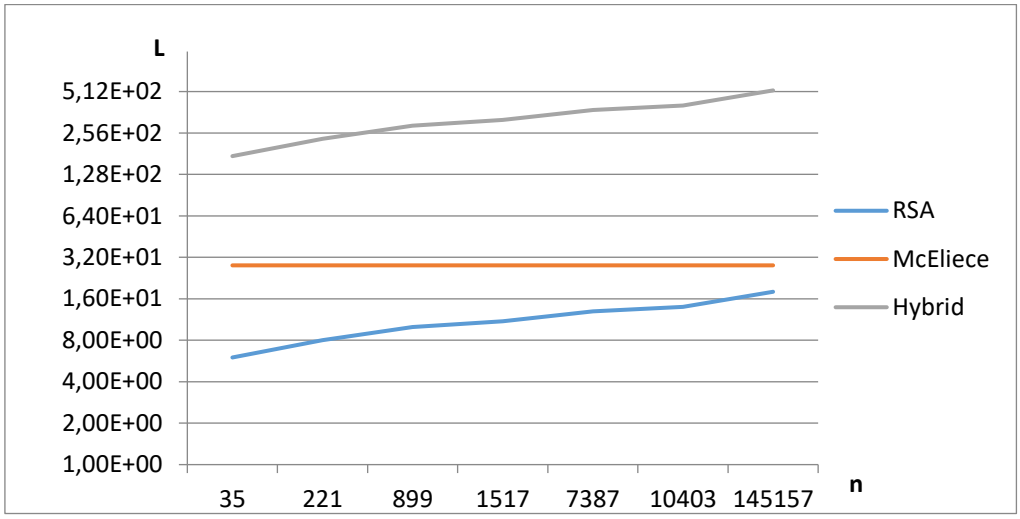


Fig. 3. Key Size Variation.

Increasing the field size *n* leads to an increase in key length for the RSA and hybrid cryptosystems, which indicates a higher level of security since larger keys make cryptanalysis more difficult. The constant key length of McEliece indicates limited adaptability of the classic McEliece algorithm to changes in field size. The hybrid cryptosystem demonstrates greater flexibility and adaptability to changes in field size, which can be beneficial in environments where security is critical. It offers a balanced solution, providing enhanced cryptographic resistance by increasing key size, but it requires more resources for computation and key storage.

The security of the hybrid cryptosystem is determined by the security of each of its components. To perform cryptanalysis of such a system, one needs to attack both McEliece and RSA. The most effective algorithms for this are Grover's algorithm [22], which can be used to attack the McEliece cryptosystem by searching for function roots or decoding sets, and Shor's algorithm [23], a quantum algorithm that allows for efficient factorization of numbers in the case of RSA.

The McEliece system is based on the use of error-correcting codes. Grover's algorithm can accelerate the search for an element in an unordered set, reducing the complexity from exponential $O(2^n)$ to $O(2^{n/2})$ due to quadratic speedup. This means that the complexity of the attack

$$T_{McEliece} = O\left(2^{\frac{2}{n}}\right)$$

will be significantly reduced, but still remains very high, making McEliece secure with large key sizes.

The security of RSA largely relies on the computational difficulty of factoring the number n for classical computers. Shor's algorithm can factorize n into prime factors in $O((log\ n)^3)$, which makes RSA vulnerable to quantum computers. To assess the resistance of RSA to attack

$$T_{RSA} = O((\log n)^3),$$

one can use the polynomial complexity of Shor's algorithm for factorization.

The resistance of the hybrid cryptosystem to quantum attacks can be evaluated as a combination of the resistance of each component:

$$T_{\text{Hybrid}} = T_{\text{McEliece}} + T_{RSA}$$
$$T_{\text{Hybrid}} = O((log\ n)^3) + O(2^{n/2}).$$

To decrypt a message in the hybrid cryptosystem, it is necessary to attack both components, as each performs different functions in the encryption process. First, the message needs to be decoded to remove the code redundancy introduced by the McEliece scheme, and then the result is decrypted using RSA to obtain the original message.

Table 3 presents the assessment of the cryptographic strength T of the systems for encrypting source data $m = 4$ characters at different values of n.

Table 3

Cryptographic Strength of Cryptosystems Against Attacks

n	$T_{McEliece}$	T_{RSA}	T_{Hybrid}
35	1,638E+04	1,349E+02	1,547E+26
221	1,638E+04	4,723E+02	8,308E+34
899	1,638E+04	9,447E+02	4,460E+43
1517	1,638E+04	1,180E+03	1,033E+48
7387	1,638E+04	2,122E+03	5,548E+56
10403	1,638E+04	2,376E+03	1,286E+61
145157	1,638E+04	5,042E+03	3,705E+78
826277	1,638E+04	7,595E+03	1,989E+87

The security of McEliece remains constant at 1.638E+04 regardless of the value of n, indicating the invariability of the key size. For the RSA system, the security increases with the increase in n, reflecting the dependency of RSA's strength on the size of the modulus. The hybrid system demonstrates the highest security, achieved by combining both systems.

Figure 4 shows the graphs of the cryptosystems' resistance to quantum attacks.

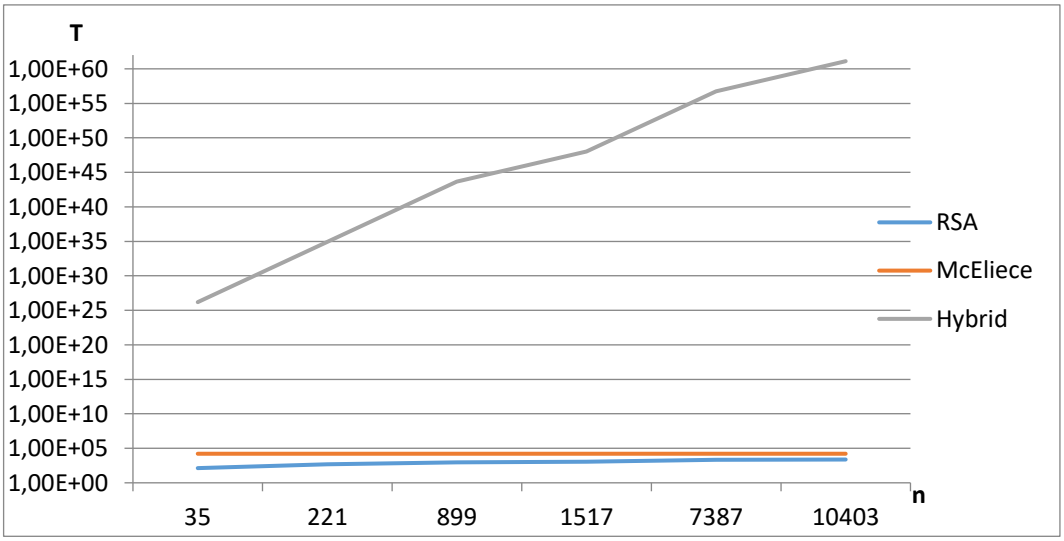


Fig. 4. Cryptosystem security as a function of n.

The hybrid cryptosystem demonstrates significantly higher cryptographic strength with increasing key size n compared to each algorithm individually. The combination of the effects of both systems allows achieving a high level of protection.

Conclusions. Both systems, McEliece and RSA, have a long history of scientific research and applications. Their cryptographic strength is based on different mathematical problems: McEliece relies on coding theory and combinatorial theory, while RSA relies on number theory and factorization. Combining them through the shared use of the value n does not contradict the mathematical principles and capabilities of both systems and also simplifies cryptographic key management.

These cryptosystems are known for their high resistance to various cryptanalytic attacks. Their integration allows for an increase in the key space by n times and complicates

approaches to breaking the ciphertext. RSA is used for encrypting short messages and digital signatures, while McEliece works well for long messages and is highly efficient in handling error correction codes. Integrating these systems allows for combining their advantages to ensure comprehensive information protection.

The conducted studies reflect important aspects of the efficiency of the proposed hybrid asymmetric cryptosystem based on codes. As the message size increases, the efficiency of data transmission increases, which is an important aspect for ensuring the speed of information exchange.

The increase in cryptographic strength of the proposed system with the increase in the Galois field size compared to the classic McEliece cryptosystem underscores the importance of the key length in cryptographic systems and their ability to protect information from cryptanalytic attacks. Specifically, increasing the key size by 6 times results in a 9.445×10^{21} times higher cryptographic strength, while changing the key data by 20 times results in a 1.214×10^{83} times higher strength. This emphasizes the importance of key length in relevant cryptographic systems and their ability to protect information from cracking attacks. The proposed hybrid cryptosystem allows for significantly improving data security by combining the advantages of both systems: McEliece provides the basic level of encryption and error correction, and the additional RSA protection enhances the overall resistance to $O\left(2^{n/2}\right) + O((log\ n)^3)$.

References

1. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signature and Public-Key Cryptosystems, *Communications of the ACM*. 1978. Vol. 21, No. 2. P. 120-126.
2. Khan M., Kamal U., Alam M., Khan H., Siddiqui S., Haque M., Parashar J. Analysis of Elliptic Curve Cryptography & RSA. *Journal of ICT Standardizatio.* 2023. Vol. 11_4. P. 355–378. doi: 10.13052/jicts2245-800X.1142.
3. Tchórzewski J., Jakóbik A. Theoretical and Experimental Analysis of Cryptographic Hash Functions. *Journal of Telecommunications and Information Technology*. 2019. Vol. 1. P.125-133. doi: 10.26636/jtit.2019.128018.
4. Amirkhanova D.S., Iavich M., Mamyrbayev O., Mamyrbayev O.Lattice-Based Post-Quantum Public Key Encryption Scheme Using ElGamal's Principles. *Cryptography. 2024.* Vol. 8, no. 3: 31. https://doi.org/10.3390/cryptography8030031.
5. Narwal E., Redhu Ritu. Mapping the Evolution of Code-Based Cryptosystems: A Comprehensive Analysis Using Science Mapping Techniques. 2024. doi: 10.9734/bpi/cpstr/v6/7513C.
6. González de la Torre M.A., Hernández Encinas L., Sánchez García J.I. Structural analysis of code-based algorithms of the NIST post-quantum call. *Logic Journal of the IGPL*. 2024. jzae071, doi: 10.1093/jigpal/jzae071.
7. Seck Boly., Cayrel P.-L., Diop I., Dragoi V.-F., Couzon K., Colombier B., Grosso V. Key-Recovery by Side-Channel Information on the Matrix-Vector Product in Code-Based Cryptosystems. *Information Security and Cryptology - ICISC 2022*. 2023. P.219-234. doi: 10.1007/978-3-031-29371-9_11.
8. Weger V., Gassner N., Rosenthal J. A Survey on Code-Based Cryptography. 2024.168 p. URL: https://arxiv.org/pdf/2201.07119.
9. Silva-García V.M., Flores-Carapia R., Alejandro Cardona-López M. A Hybrid Cryptosystem Incorporating a New Algorithm for Improved Entropy. *Entropy*. 2024. Vol. 26, no. 2. P. 154. doi: 10.3390/e26020154.
10. Suhael S., Ahmed Z., Hussain A. Proposed Hybrid Cryptosystems Based on Modifications of Playfair Cipher and RSA Cryptosystem. *Baghdad Science Journal*. 2023. doi: 10.21123/bsj.2023.8361.
11. Garms L., Paraïso T., Hanley N., Khalid A., Rafferty C., Grant J., Newman J., Shields A., Cid C., O'Neill M. Experimental Integration of Quantum Key Distribution and Post-

Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem. *Advanced Quantum Technologies*. 2024. Vol. 7. doi: 10.1002/qute.202300304.

12. McEliece, R.J. A Public-Key Cryptosystem Based on Algebraic Coding Theory. *DSN Progress Report*. 1978. Vol. 42(44). P. 114-116.
13. Couvreur A., Mora R., Tillich J.-P. A New Approach Based on Quadratic Forms to Attack the McEliece Cryptosystem. 2023. doi: 10.1007/978-981-99-8730-6_1.
14. Lau T., Tan C.H. On the design and security of Lee metric McEliece cryptosystems. *Designs, Codes and Cryptography.* 2022. Vol. 90. doi:10.1007/s10623-021-01002-2.
15. Bindal E., Singh A. Secure and Compact: A New Variant of McEliece Cryptosystem. *IEEE Access*. 2024. P. 1-1. doi:10.1109/ACCESS.2024.3373314.
16. Parashar A. Enhanced McEliece Algorithm for Post-Quantum Cryptosystems. 2024. doi: 10.13140/RG.2.2.22002.93125.
17. Mariot L., Picek S., Yorgov, R. On McEliece-Type Cryptosystems Using Self-Dual Codes With Large Minimum Weight. *IEEE Access*. 2023. P. 1-1. doi: 10.1109/ACCESS.2023.3271767.
18. Anuradha M., Loganathan S., Suseela G., Selvan M.P., Nalini M., Chitra D.D, Hybrid Multiple Cryptography for Data Encryption. *2023 8th International Conference on Communication and Electronics Systems (ICCES)*. 2023. P. 596-603. doi: 10.1109/ICCES57224.2023.10192838.
19. Jintcharadze E., Iavich M. Hybrid Implementation of Twofish, AES, ElGamal and RSA Cryptosystems. *2020 IEEE East-West Design & Test Symposium (EWDTS)*. 2020. P. 1-5, doi: 10.1109/EWDTS50664.2020.9224901.
20. Jian M.-S., Cheng Y.-E., Shen C.-H. Internet Of Things (IOT) Cybersecurity based on the Hybrid Cryptosystem. *2019 21st International Conference on Advanced Communication Technology (ICACT)*. 2019.P. 176-181, doi: 10.23919/ICACT.2019.8701957.
21. Кузнецов О.О., Горбенко Ю.І., Кіян А.С., Уварова А.О., Кузнецова Т.Ю.Порівняльні дослідження та аналіз ефективності гібридної кодовоїкриптосистеми. Радіотехніка. 2018. Вип. 195. С. 61-69.
22. Opiłka F., Niemiec M., Gagliardi M., Kourtis M. A., 2024. Performance Analysis of Post-Quantum Cryptography Algorithms for Digital Signature. *Applied Sciences*. 2024. Vol. 14, no. 12: 4994. doi: 10.3390/app14124994.
23. Regev, Oded. An Efficient Quantum Factoring Algorithm. 2023. URL: https://arxiv.org/pdf/2308.06572.

ГІБРИДНА АСИМЕТРИЧНА КРИПТОСИСТЕМА НА ОСНОВІ КОДІВ

А.Я. Давлетова

Західноукраїнський національний університет,
11, Львівська вул., м.Тернопіль, 46020, Україна;
email: a7davletova@gmail.com

Робота присвячена вирішенню актуальної задачі забезпечення надійного захисту інформації в умовах збільшення обсягів даних та зростання кількості кіберзагроз. Традиційні криптографічні системи, хоча і є досить надійними, можуть виявитися вразливими до нових типів атак, особливо до квантових. Це підкреслює необхідність пошуку та дослідження більш стійких методів шифрування. У роботі запропонована гібридна криптосистема, що поєднує систему McEliece та алгоритм шифрування RSA. Такий підхід дозволяє використати переваги обох методів: високий рівень безпеки RSA, заснований на складності факторизації великих чисел, та стійкість McEliece до квантових атак завдяки складності декодування довільних лінійних кодів. Особливістю запропонованої гібридної системи є використання полів Галуа *GF(p)* для всіх операцій, що забезпечує додатковий рівень захисту та гнучкість. Інтеграція асиметричних криптоалгоритмів, стійкість яких базується на вирішенні різних математичних задач, забезпечує підвищення надійності та безпеки запропонованої системи. Використання спільного параметра n для генерації ключів також спрощує управління ними та розширює словник у n разів. Таке рішення поєднує в собі захист від помилок та криптографічну безпеку, що робить його потужним інструментом для захисту даних в умовах обміну інформацією через потенційно ненадійні канали передачі. Дослідження, проведені в рамках роботи, спрямовані на аналіз ефективності та безпеки запропонованої гібридної криптосистеми. Особлива увага приділена таким характеристикам, як відносна швидкість передачі інформації, довжина шифротексту, обсяг ключів та стійкість до криптоаналізу. Результати демонструють переваги гібридної системи у порівнянні із використанням кожного з алгоритмів окремо.

Ключові слова: криптосистема McEliece, алгоритм шифрування RSA, скінчені поля Галуа, гібридна криптосистема, стійкість до криптоаналізу.

DOI 10.15276/imms.v14.no1-2.24
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 24-36

МЕТОД ВИЯВЛЕННЯ ФОТОМОНТАЖУ НА ЦИФРОВОМУ ЗОБРАЖЕННІ

А.А. Кобозєва[1], Б.Г. Єнакієв[2]

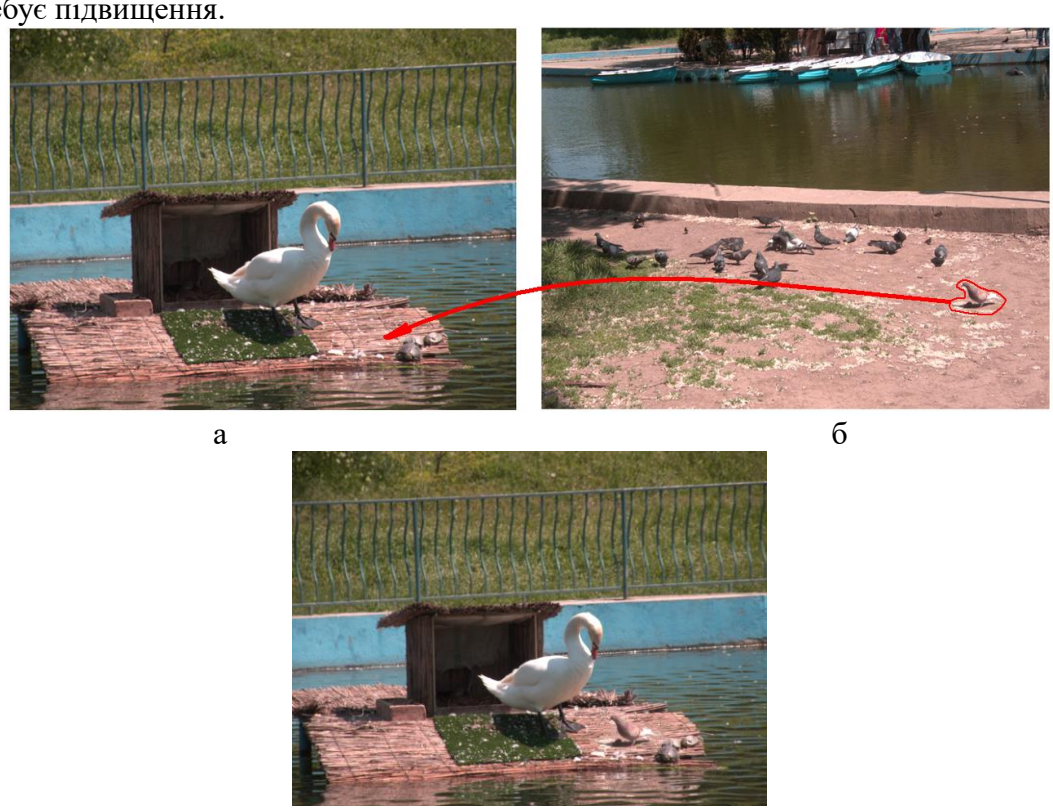
[1]Одеський національний університет імені І.І.Мечникова,
2, Дворянська вул., м.Одеса, 65082, Україна,
email: alla_kobozeva@ukr.net
[2]Національний університет «Одеська політехніка»,
1, Шевченка пр., м.Одеса, 65044, Україна;
email: enakievb@gmail.com

Цілісність інформаційного контенту, зокрема цифрового зображення, що розглядається в роботі, є одним з критеріїв його захищеності. Одним з найпоширеніших на сьогодні та таким, що легко реалізується за допомогою існуючих графічних редакторів (PhotoShop, Gimp та ін.) способів фальсифікації – порушення цілісності цифрових зображень є фотомонтаж, в ході якого одне зображення створюється з декількох. Не дивлячись на те, що задача виявлення фотомонтажу є предметом дослідження вчених в галузі інформаційної безпеки по всьому світу, вона залишається надзвичайно актуальною на сьогоднішній день, оскільки не є остаточно вирішеною: не існує універсальних експертних методів, які в змозі навіть детектувати наявність «чужорідної» частини – вклейки у будь-якому випадку фотомонтажу, крім того ефективність існуючих методів потребує підвищення навіть в обмежених умовах їх застосування. В роботі представлений новий поліноміальний ступеня 2 експертний метод, який на основі аналізу властивостей матриці найменших сингулярних чисел блоків, що ставиться у відповідність матриці цифрового зображення, дає змогу відокремити оригінальне зображення від такого, цілісність якого порушена, а також локалізувати область, що містить в собі «вклейку» – частину іншого зображення. Представлений метод базується на встановлених відмінностях властивостей матриці найменших сингулярних чисел блоків для цифрових зображень, що зберігаються в різних форматах – з втратами та без втрат, які знайшли своє відображення в запропонованому в роботі методі відокремлення зображень в різних форматах збереження, що може використовуватися як окремо, так і як складова розробленого методу виявлення фотомонтажу у випадку, коли означене фальсифіковане зображення складається з частин зображень, збережених з втратами та без втрат. Встановлено, що запропонований експертний метод забезпечує підвищення ефективності процесу виявлення факту наявності фотомонтажу в порівнянні з сучасним методом-аналогом.

Ключові слова*:* цифрове зображення, фотомонтаж, сингулярне число, матриця найменших сингулярних чисел, вклейка

Вступ. Інформаційна сфера сьогодні стала базовою для розвитку всіх інших сфер людського життя: економічної, політичної, дипломатичної тощо [1]. Природнім наслідком цього є те, що питання захисту інформації стає одним з найактуальніших питань не тільки сучасної науки, а й сучасного життя в цілому. Одним з критеріїв захищеності інформації є її цілісність, що полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом [2,3]. Але сучасне інформаційне поле, як правило, не надає гарантій цілісності циркулюючої в ньому інформації [1], що приводе до актуальності наявності методів, алгоритмів, засобів для ефективного відокремлення оригінального контенту від зміненого, спотвореного, зокрема цифрових зображень, що розглядаються в роботі. Ця актуальність для нас стала критичною під час війни України проти агресії Росії, під час інформаційної війни, що розвернула країна-агресор, поширюючи різноманітні фото-, відеофейки в світовому інформаційному просторі, довіра до яких створює хибне уявлення, розуміння наявних

подій та їх результатів. Одним з найпоширеніших на сьогодні та таким, що легко реалізується за допомогою існуючих графічних редакторів (PhotoShop, Gimp та ін.) способів фальсифікації – порушення цілісності цифрових зображень є фотомонтаж (рис.1), коли одне цифрове зображення (ЦЗ) створюється з декількох [4-7]. Не дивлячись на те, що задача виявлення фотомонтажу є предметом дослідження вчених в галузі інформаційної безпеки по всьому світу, які застосовують при цьому різноманітні теоретичні (математичні) базиси (дискретне вейвлет-перетворення і гистограми дискримінаційних робастних локальних двійкових шаблонів [4]; модель згорткової нейронної мережі [5], властивості параметрів нормального сингулярного розкладання блоків матриці ЦЗ [6] тощо), вона не є остаточно вирішеною: не існує універсальних експертних методів, які в змозі навіть детектувати наявність «чужорідної» частини – вклейки у будь-якому випадку фотомонтажу, до того ж ефективність існуючих методів потребує підвищення.



а б

в

Рис.1. Ілюстрація застосування для ЦЗ фотомонтажу: а, б – оригінальні ЦЗ; в – результат проведеного фотомонтажу

Метою роботи є підвищення ефективності процесу виявлення порушення цілісності цифрового зображення шляхом розробки методу виявлення факту фотомонтажу.

Для досягнення поставленої мети в роботі вирішуються наступні *задачі*:

1. Визначити та обґрунтувати доцільність математичного об’єкту, що ставиться у відповідність ЦЗ, для використання його в процесі експертизи цілісності зображення;
2. Дослідити властивості математичного об’єкту, визначеного в задачі 1, що ставиться у відповідність ЦЗ;
3. На основі встановлених властивостей математичного об’єкту, визначеного в задачі 1, розробити метод відокремлення ЦЗ в різних форматах збереження: з втратами та без втрат;
4. Розробити метод виявлення фотомонтажу для випадку, коли фотомонтаж містить частини ЦЗ в різних форматах збереження;

5. Провести оцінку ефективності, в тому числі, порівняльну розробленого методу виявлення фотомонтажу.

Об'єктом дослідження в роботі є процеси порушення цілісності ЦЗ.

Предметом дослідження є методи виявлення фотомонтажу в ЦЗ.

Розробка методу відокремлення цифрових зображень в різних форматах збереження. Останнім часом переважна більшість методів, що працюють з ЦЗ, кадрами цифрового відео, є блоковими, тобто такими, що здійснюють аналіз/обробку зображення/кадра поблоково, попередньо проводячи відповідну розбивку матриці зображення. Частіше за все – це стандартна розбивка [8] на непересічні квадратні блоки одного розміру, хоча це не обов'язково. Блокова обробка зображень має свої переваги, основна з яких – незначна обчислювальна складність. Дійсно, якщо обробляється цифровий контент (зображення, кадр відео) з $n \times n$-матрицею, яка попередньо розбита на непересічні $l \times l$-блоки, то незалежно від специфіки самого алгоритму, його обчислювальна складність буде визначатися кількістю блоків, тобто становити

$$k \times \left\lceil \frac{n}{l} \right\rceil \times \left\lceil \frac{n}{l} \right\rceil = O\left(n^2\right)$$

операцій, де k – кількість операцій для обробки одного блоку, яка ніяк не залежить від розміру ЦЗ, $\lceil g \rceil$ – ціла частина від аргументу. Враховуючи вищенаведене, експертиза ЦЗ в розроблюваному методі передбачає попередню розбивку його матриці на квадратні непересічні блоки одного розміру. В роботі передбачається, що фотомонтаж формується наступним чином. Використовуються два ЦЗ в різних форматах збереження: з/без втрат. Одне з них відіграє роль основного, а друге такого, з якого береться частина, яка переноситься на перше зображення, створюючи на ньому заміщуючу область – вклейку (рис.1). Для виявлення результатів фотомонтажу в таких умовах ключовим моментом є наявність інструменту для відокремлення ЦЗ в різних форматах збереження. Не обмежуючи спільності міркувань, для простоти подальшого викладу будемо вважати, що формально будь-яке ЦЗ під час експертизи представляється одною $n \times m$-матрицею F. Якщо ЦЗ є кольоровим, то, залежно від схеми збереження, F може бути або матрицею яскравості (схема YUV), або одною з матриць кольорів (схема RGB). Останнім часом дуже добре для вирішення задач інформаційної безпеки зарекомендував себе загальний підхід до аналізу стану й технології функціонування інформаційних систем (ЗПАІС) [9], заснований на теорії збурень та матричному аналізі, відповідно до якого зміна стану будь-якої інформаційної системи, частковим випадком якої є ЦЗ, цифрове відео, представляється сукупністю збурень повного набору формальних параметрів, що визначають матрицю, яка ставиться у відповідність інформаційній системі. Один з повних наборів складається з сингулярних чисел (СНЧ) і сингулярних векторів матриці, отриманих за допомогою нормального сингулярного розкладання, що визначається однозначно для матриці, яка не має кратних СНЧ [10]. З урахуванням цього, а також того, що матриця оригінального ЦЗ, як правило, не має кратних СНЧ, в якості основних аналізованих параметрів для рішення задачі, що розглядається в роботі, будемо розглядати СНЧ матриці (блоків матриці) зображення, які є добре обумовленими, на відміну від сингулярних векторів, які в межах одної матриці можуть бути як добре, так і погано обумовленими [11].

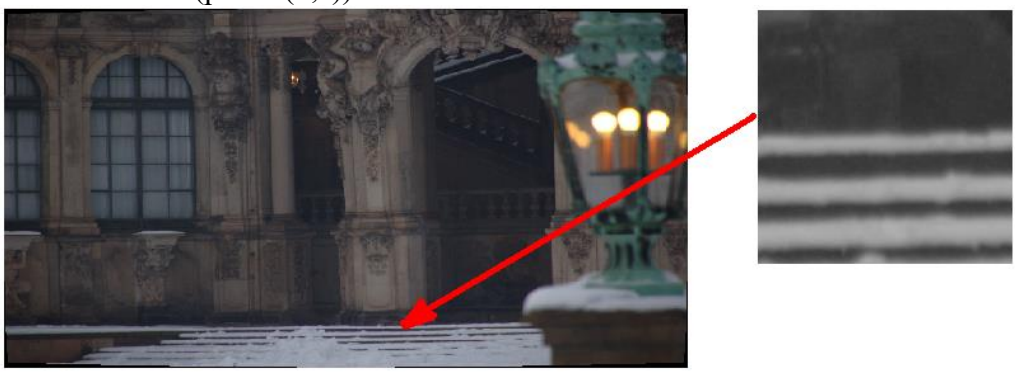
Матриці F ЦЗ поставимо у відповідність матрицю M найменших сингулярних чисел блоків (МНСБ) за наступним правилом. Матриця F розбивається попередньо стандартним чином на непересічні $l \times l$-блоки. В МНСБ M, розмір якої $\left\lceil \frac{n}{l} \right\rceil \times \left\lceil \frac{m}{l} \right\rceil$, кожний елемент $m_{ij}, i = \overline{1, \left\lceil \frac{n}{l} \right\rceil}, j = \overline{1, \left\lceil \frac{m}{l} \right\rceil}$, відповідає блоку B ЦЗ, визначаючи в B кількість СНЧ, менших заданого порога T, значення якого очевидно буде залежати від

розміру блоку l. При цьому СНЧ B визначаються за допомогою сингулярного розкладання [11]:

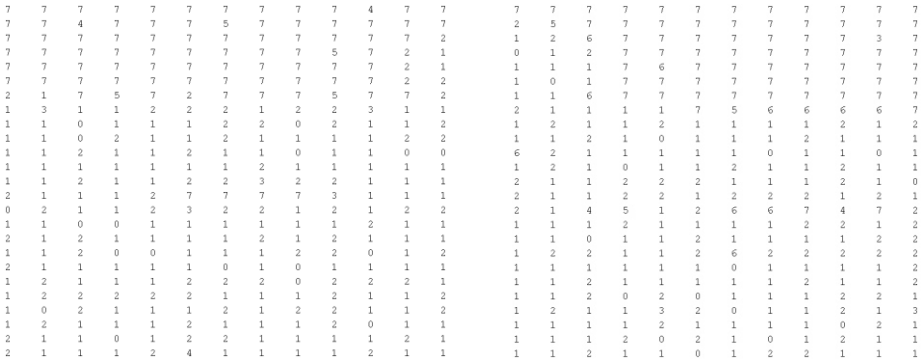
$$B = U\Sigma V^T, \quad (1)$$

де U, V – ортогональні матриці, стовпці яких u_i, v_i, $i = \overline{1,l}$, визначають ліві і праві сингулярні вектори B відповідно, а $\Sigma = diag(\sigma_1, \sigma_2, ..., \sigma_l)$, де $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_l \geq 0$ – СНЧ. СНЧ разом з відповідними лівим і правим сингулярними векторами утворюють сингулярні трійки для блоку B ЦЗ: (σ_i, u_i, v_i), $i = \overline{1,l}$.

Відомо, що стиск ЦЗ з втратами (незалежно від конкретики використовуваного алгоритму стиску) приводить до зменшення/знищення високочастотної (можливо, і середньочастотної, що залежить від коефіцієнту стиску) складової зображення. При цьому високочастотним складовим відповідають, головним чином, сингулярні трійки (σ_i, u_i, v_i) з найменшими СНЧ [9]. Враховуючи це, стиск призводе до зменшення найменших СНЧ ЦЗ (блоків ЦЗ), можливо, аж до нуля, що раніше вже зазначалося як в [9], так і в [6]. Однак на практиці «чистих» нулів, як правило, не буде, оскільки в процесі обчислень в системі чисел з плаваючою точкою виникає обчислювальна похибка, зокрема, при відновленні ЦЗ після стиску, і відповідні (найменші за значенням) СНЧ будуть порівнянними з похибкою округлення, що повинно відбитися на значеннях елементів МНСЧ, і робить доцільнім при її побудові враховувати саме «малість» значень СНЧ, а не їх рівність нулю, як пропонувалося в [6]. Очевидно, що МНСЧ для ЦЗ у різних форматах збереження (з/без втрат) будуть відрізнятися між собою своїм вмістом (рис.2 (б,г)).



а



б

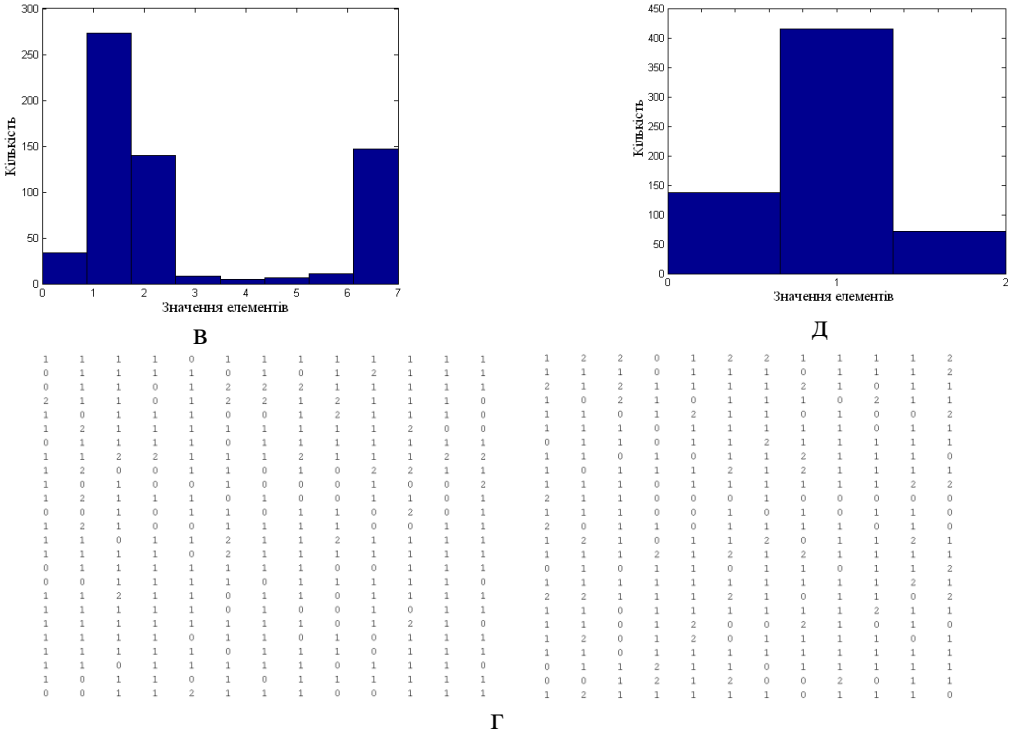


Рис.2. Ілюстрація відмінності МНСЧ для відповідних ЦЗ в різних форматах збереження (T=0.5; l=8): а – ЦЗ1 розміром 200×200 пікселів в форматі Jpeg (коефіцієнт якості QF=75); б – МНСБ для ЦЗ1; в – гістограма значень МНСБ для ЦЗ1; г – МНСБ для ЦЗ2 в форматі Tif, відповідного ЦЗ1; д – гістограма ень МНСБ для ЦЗ2

Для блоків ЦЗ в форматі без втрат СНЧ, значення яких менші за T, як правило, менше, ніж в блоках ЦЗ в форматі з втратами, на що наочно вказують гістограми МНСБ (рис.2(в,д)). Таким чином, саме МНСЧ буде тим математичним об'єктом, що ставиться у відповідність ЦЗ, аналіз якої буде використовуватися в процесі експертизи цілісності зображення, тобто вирішує задачу 1 з переліку задач дослідження.

Враховуючи все вищенаведене, основні кроки методу відокремлення ЦЗ в різних форматах збереження (з/без втрат) виглядають наступним чином:

Крок 1. Матриця F ЦЗ розміром $n\times m$, що піддається експертизі цілісності, розбивається стандартним чином на непересічні $l\times l$-блоки B_{ij}, де i – номер блокового рядка, j – номер блокового стовпця, на перерізі яких знаходиться блок, $i=\overline{1,\left[\frac{n}{l}\right]}$, $j=\overline{1,\left[\frac{m}{l}\right]}$ (відлік починається з лівого верхнього кута ЦЗ) (рис.3).

Крок 2. (Побудова матриці M найменших сингулярних чисел блоків).

Для визначення елемента m_{ij}, $i=\overline{1,\left[\frac{n}{l}\right]}$, $j=\overline{1,\left[\frac{m}{l}\right]}$ матриці M розміру $\left[\frac{n}{l}\right]\times\left[\frac{m}{l}\right]$:

2.1. Побудувати сингулярне розкладання (1) для відповідного блоку B_{ij}:

$$B_{ij}=U\Sigma V^T$$

з якого визначити сингулярні числа B_{ij}: $\sigma_1\geq\sigma_2\geq...\geq\sigma_l\geq0$.

2.2. Визначити кількість $K\in\{0,1,2,...,l\}$ СНЧ B_{ij}, для яких має місце: $\sigma_t<T$,

де T – порогове значення, що визначається експериментальним шляхом для кожного l.

2.3. Визначення елемента m_{ij}: $m_{ij} = K$.

Крок 3. Побудувати гістограму значень елементів матриці M; визначити моду $mod\,M$ гістограми.

Крок 4.(Експертний висновок).

Якщо $mod\,M \geq T_{mod\,\mathrm{T}}$ *то* ЦЗ збережене в форматі з втратами.

Якщо $mod\,M = 0$ *то* ЦЗ збережене в форматі без втрат.

Якщо $\left(1 \leq mod\,M \leq T^1_{mod}\right) \& \left(\exists m_{ij} > T^2_{mod}\right)$ *то* ЦЗ збережене в форматі з втратами

Якщо.. $\left(1 \leq mod\,M \leq T^1_{mod}\right) \& \left(\neg\exists m_{ij} > T^2_{mod}\right)$ *то* ЦЗ збережене в форматі без втрат

де T_{mod}, T^1_{mod}, T^2_{mod} встановлюються експериментально для кожного l.

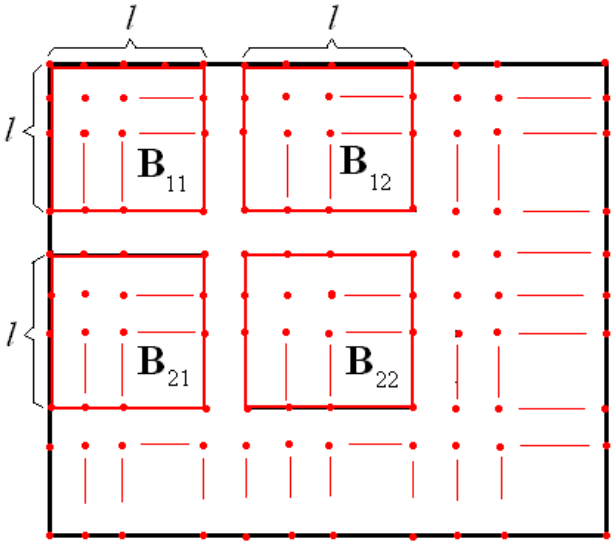


Рис.3. Розбивка матриці F ЦЗ на $l \times l$-блоки для побудови матриці M найменших СНЧ блоків

Експериментально встановлено рекомендовані значення параметрів методу відокремлення ЦЗ в різних форматах збереження (з втратами, без втрат) для l=8 (враховуючи, що найпопулярнішими і найпоширенішими алгоритмами стиску ЦЗ з втратами є JPEG та JPEG2000, що використовують 8×8-блоки):

$$T = 0.3;\ T_{mod} = 3;\ T^1_{mod} = 2;\ T^2_{mod} = 4.$$

На рис.4,5 продемонстровані результати роботи програмного продукту, що реалізує алгоритм, відповідний запропонованому методу (для вказаних значень параметрів).

Рис. 4. Зображення у форматі без втрат та його гістограма

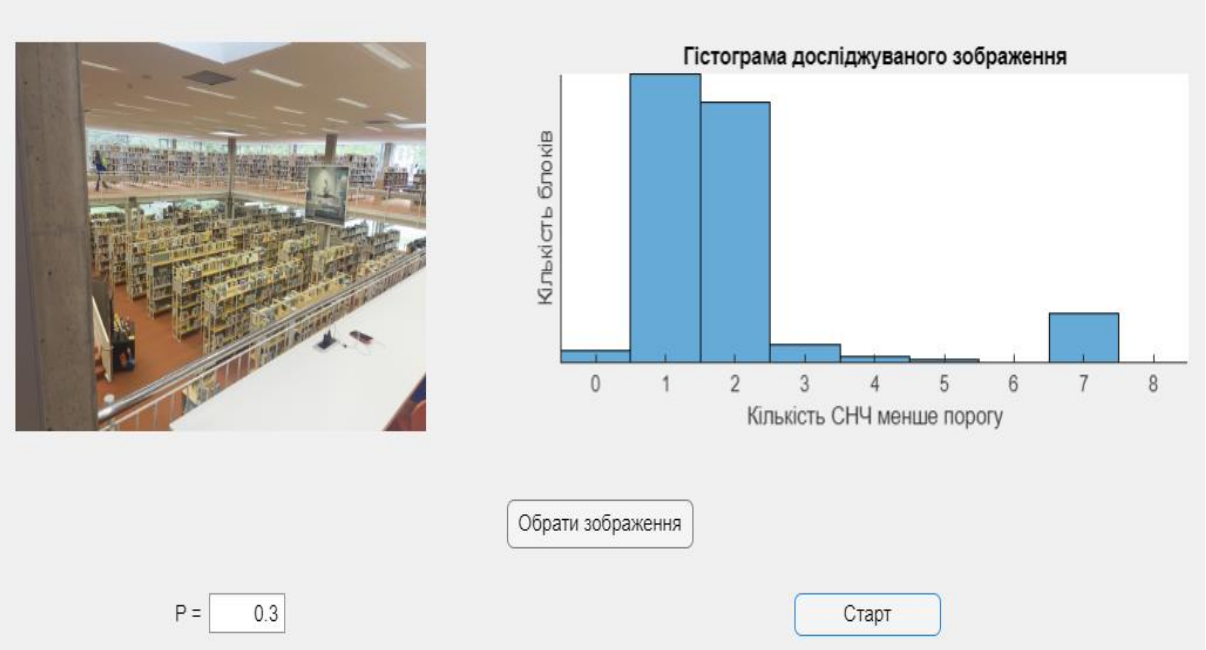


Рис. 5. Зображення у форматі з втратами та його гістограма

Гістограма першого зображення має моду, що дорівнює 0, тому однозначно відповідає ЦЗ в форматі без втрат (рис.4), мода гістограми для другого зображення дорівнює 1 і при цьому має ненульові стовпчики для аргументів 5 і 7, що говорить про формат ЦЗ з втратами (рис.5). І перший, і другий випадки відповідають дійсності.

Метод виявлення фотомонтажу. Використовуючи отримані вище відмінності між ЦЗ, що були збережені у форматі з втратами, від зображень у форматі без втрат, запропоновано метод виявлення фотомонтажу з локалізацією вклейки – фрагменту стиснутого зображення на оригінальному фоновому зображенні в форматі без втрат.

Сформуємо множину X, яку поставимо у відповідність матриці M найменших СНЧ блоків ЦЗ, наступним чином. Серед M знаходимо максимальний елемент: $X_a = \max\limits_{i,j} m_{ij}$. Через те, що значення елементів матриці M не є унікальними між собою,

значення X_a може мати певна кількість елементів m_{ij}. Ці і тільки ці елементи M увійдуть у множину X.

Експериментально встановлено, що якщо потужність множини X буде меншою за п'ять (при використанні блоків розміром l=8), то ЦЗ з матрицею F не містить вклейки.

Нехай кількість елементів в X неменша за 5. Оскільки стиск цифрового зображення з втратами не зменшує значення його матриці найменших сингулярних чисел, то можна припустити, що деякі зі знайдених елементів m_{ij} із X належать вклейці. Розглянемо околи O розміром $L\times L$ (розмір околу L визначається експериментально) навколо кожного знайденого елементу $m_{ij}=X_a$ з множини X. Серед побудованих околів визначимо той, що включає в себе найбільшу кількість елементів $m_{ij} \in X$ з усіх.

Для того, щоб пересвідчитись в тому, що знайдений фрагмент O матриці M відповідає частині досліджуваного ЦЗ, що містить вклейку, отриману з ЦЗ у форматі з втратами, розраховується різниця S між середніми значеннями елементів матриці M та визначеного фрагменту O:

$$S = \left|A_1 - A_2\right|, \tag{4}$$

де A_1 – середнє арифметичне значень елементів матриці M, A_2 – середнє арифметичне значень елементів O.

Експериментально встановлено, що значення S у випадку, коли окіл O не містить вклейку, що є частиною ЦЗ в форматі з втратами, зазвичай становить менше ніж 0.2. Відповідно, якщо знайдене значення S буде більше ніж 0.2, то це може свідчити про наявність неоригінальних частин в O.

Однак вклейка може бути незначного розміру в порівнянні з розміром околу O. Це може призвести до того, що в цьому випадку значення S буде меншим за 0.2, і вклейку не буде зафіксовано. Для покращення даної ситуації необхідна додаткова перевірка знайденого фрагменту O, щоб він вважався «чистим». Для цього водиться параметр P, який встановлює відсоток елементів X_a, які належать фрагменту O, відносно їх загальної кількості в матриці M:

$$P = \frac{X_l}{X_g} \cdot 100\%, \tag{5}$$

де X_l – кількість елементів зі значенням X_a у фрагменті O, X_g – кількість елементів X_a у всій матриці M.

Експериментально встановлено, що для того, щоб фрагмент O, пройшовши перевірку, вважався «чистим», значення P має становити менше 60%.

Враховуючи все вищенаведене, основні кроки запропонованого методу виявлення фотомонтажу на цифрових зображеннях виглядають наступним чином:

Крок 1, Крок 2 відповідають методу відокремлення ЦЗ в різних форматах збереження.

Крок 3. Визначити: $X_a = \max\limits_{i,j} m_{ij}$ – максимальне значення елементів МНСЧ M.

Крок 4. З матриці M найменших сингулярних чисел блоків формується множина X елементів, значення яких дорівнюють X_a.

Крок 5. Перевірка загальної кількості елементів множини X

Якщо $\left|X\right| < 5$, де $\left|X\right|$ – потужність множини X,

то ЦЗ не містить вклейку, *кінець експертизи* (перехід на крок 10)

Крок 6. Побудова околів O розміром $L\times L$ для кожного значення $m_{ij} \in X$.

Крок 7. З побудованих на кроці 6 околів визначити окіл $\overline{O}$, який містить найбільшу кількість елементів множини X.

Крок 8. Розрахунок значень S (4) та P (5) для подальшого аналізу обраного фрагменту $\overline{O}$.

Крок 9. (Експертний висновок)

Якщо $S > 0.2$ *то* ідентифіковано вбудований фрагмент (перехід на крок 10).

Якщо $P > 60\%$ *то* ідентифіковано вбудований фрагмент (перехід на крок 10)

Якщо $(S \le 0.2) \& (P \le 60\%)$ *то* ЦЗ не містить вклейку

Крок 10. Кінець експертизи

На рис.6,7 продемонстрована робота програмного продукту, що реалізує розроблений метод з пороговим значенням T=0.3, L=100, результатом чого є правильне виявлення факту наявності фотомонтажу та локалізація безпосередньо вклейки на зображенні.

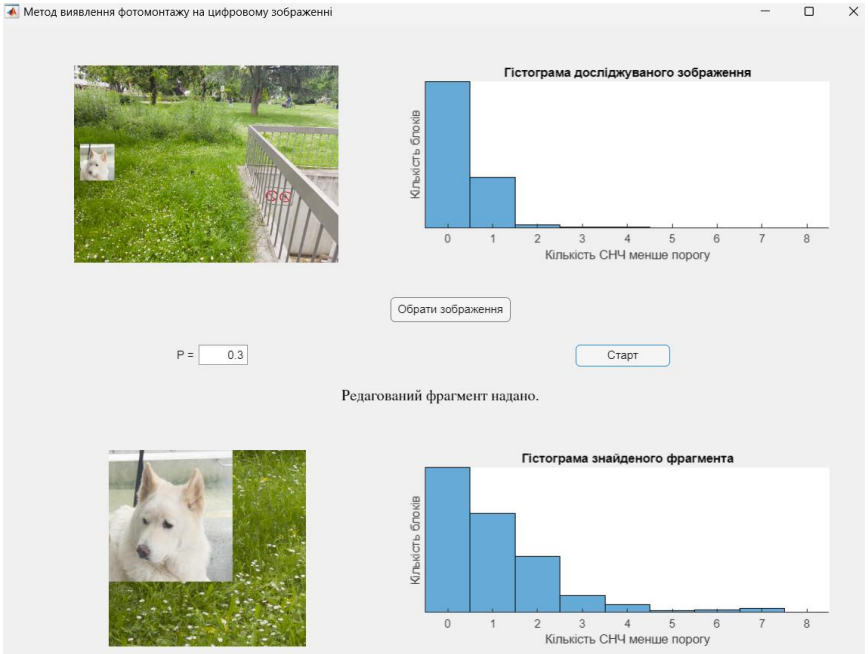


Рис.6. Результат роботи програмного продукту, що реалізує розроблений метод, при виявленні наявного фотомонтажу

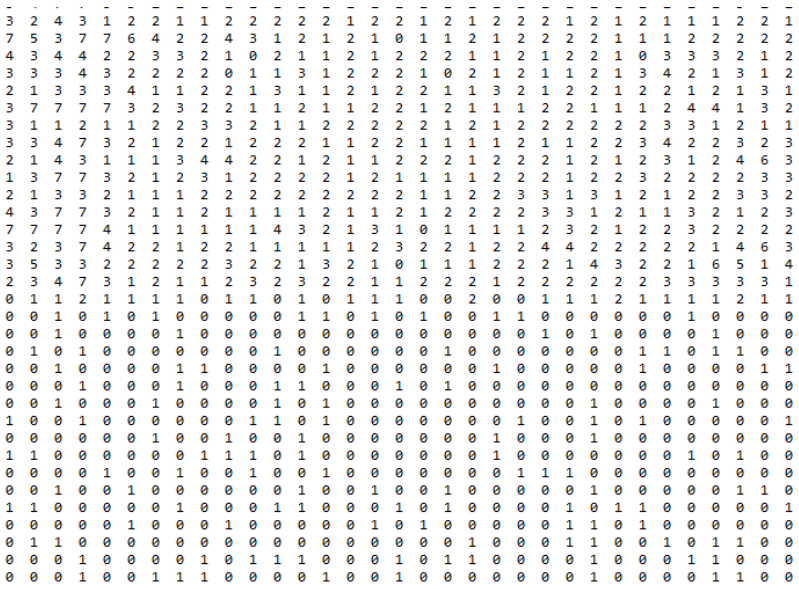


Рис. 7. Фрагмент матриці найменших сингулярних чисел блоків на межі перетину фонового зображення зі знайденою вставкою

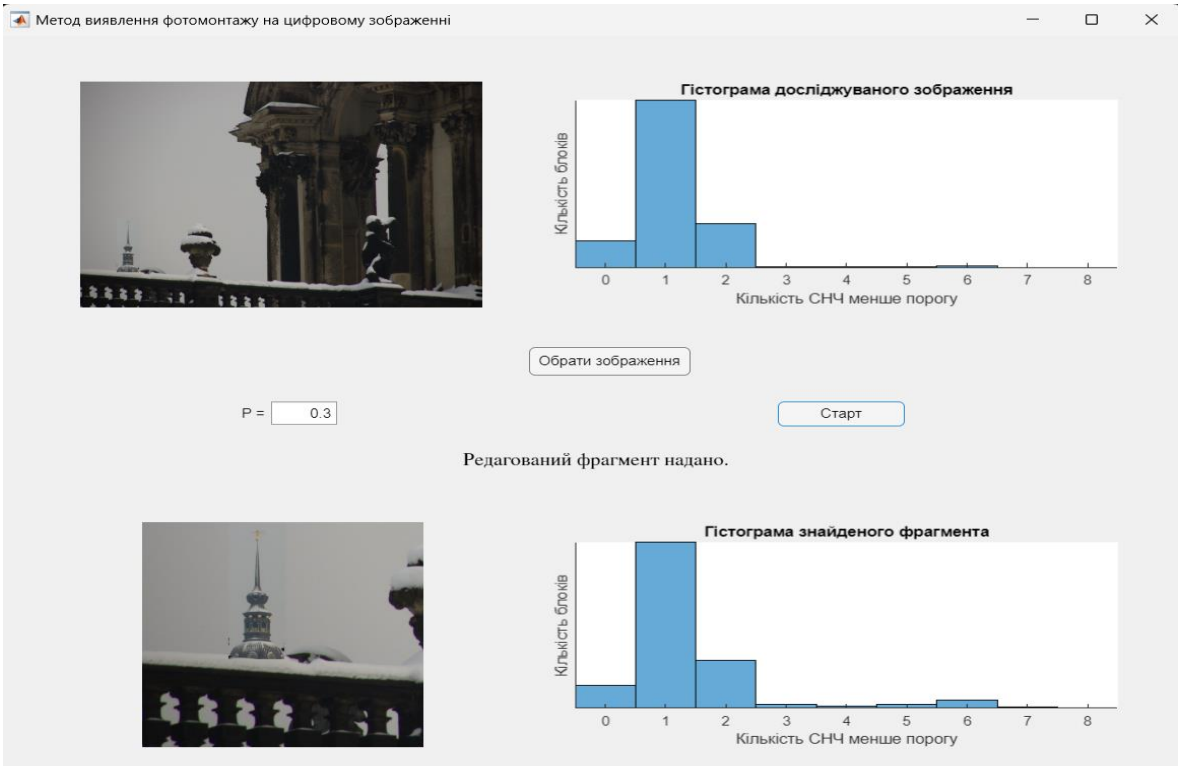
Результатом роботи розробленого методу є фрагмент досліджуваного зображення розміром 800×800 пікселів, який відповідає обраному фрагменту матриці найменших сингулярних чисел блоків, а також сам обраний фрагмент матриці.

Програмна реалізація та оцінка ефективності розробленого методу виявлення фотомонтажу. В процесі дослідження ефективності роботи запропонованого методу було створено програмний продукт, який дозволяє користувачу обирати зображення та встановлювати порогове значення *T* для проведення експертизи цілісності.

На рис.8,9 можна побачити демонстрацію типових результатів для конкретних ЦЗ (підданого фотомонтажу (рис.8), та оригінального (рис.9)) розробленого програмного продукту.

а

б



в

Рис. 8. Результат роботи програмного продукту, що реалізує розроблений метод, у випадку, коли досліджуване ЦЗ містить вклейку: а – фонове ЦЗ; б – ЦЗ, з якого береться вклейка; в – результат виявлення фотомонтажу та локалізації області вклейки

В якості фонового зображення на рис.8 фігурує ЦЗ (рис.8(а)) у форматі PNG. Вклейка, а саме виділена у червоний прямокутник башта, була взята з ЦЗ у форматі JPEG з коефіцієнтом якості *QF*=80 (рис.8(б)). Вклейка була успішно знайдена, виділений фрагмент надано (рис.8(в)).

На рис.9 представлені результати експертизи оригінального ЦЗ (рис.8(а)), де не зафіксовано жодних змін на зображенні. При порівнянні гістограм досліджуваних зображень (рис.8(в) та рис.9) можна помітити, що на гістограмі зображення зі вставкою наявна значна кількість шісток та сімок, в той час як на гістограмі зображення без вставки ці елементи відсутні.

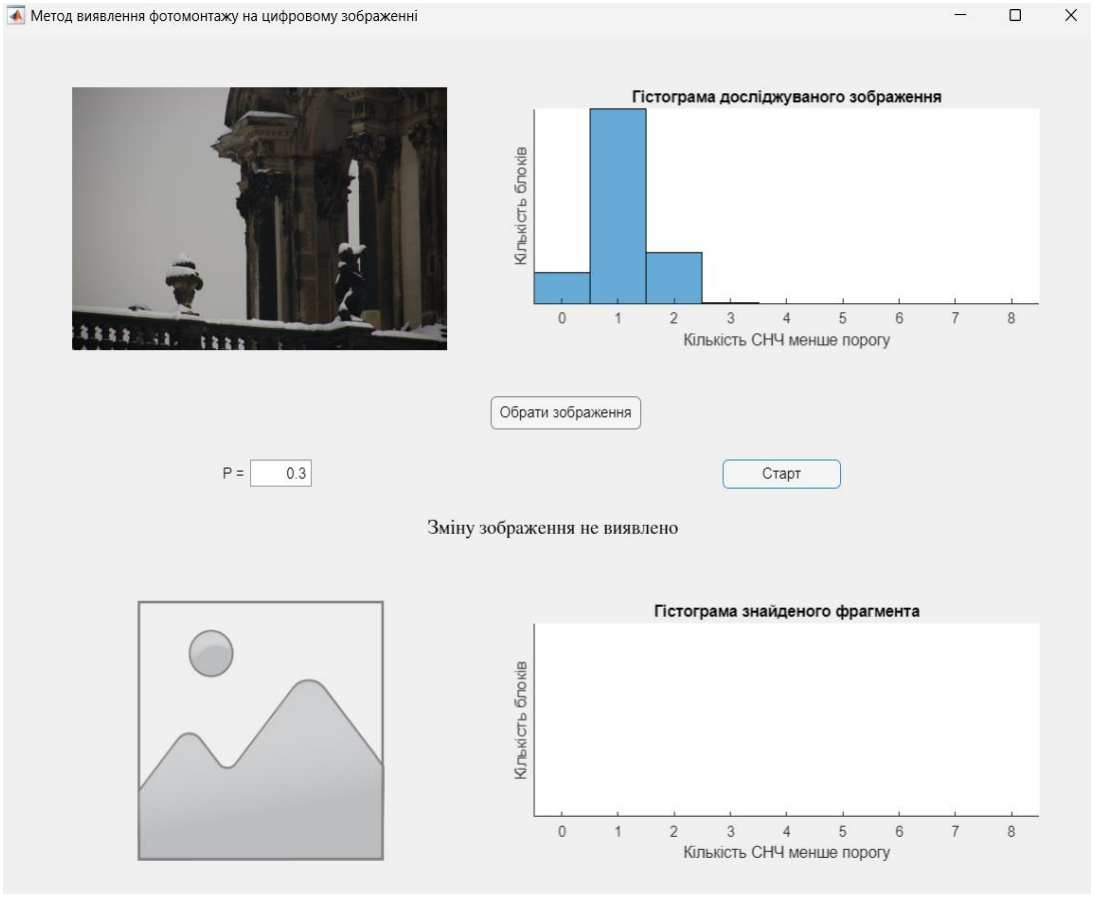


Рис.9. Результат роботи програмного продукту, що реалізує розроблений метод, у випадку, коли досліджуване ЦЗ є оригінальним

Для оцінки ефективності розробленого методу виявлення фотомонтажу був проведений обчислювальний експеримент, в якому було задіяно 100 оригінальних ЦЗ, отриманих як професійними, так і непрофесіональними відеокамерами, які піддавалися фотомонтажу. Оригінальні і спотворені ЦЗ піддавалися експертизі за допомогою розробленого методу. Кількісними результатами проведення експерименту стали помилки 1-го (спотворене ЦЗ ідентифікувалося як оригінальне) і 2-го (оригінальне ЦЗ ідентифікувалося як спотворене) роду. Для порівняльної оцінки ефективності був обраний сучасний метод-аналог, запропонований в [6], оскільки він має подібну до розробленого область застосування і схожий математичний апарат, заснований на аналізі СНЧ блоків матриці ЦЗ.

Результати проведеного обчислювального експерименту представлені в табл.1 (тут помилки 1-го і 2-го роду для методу [6] рахувалися як середні значення відповідних помилок для всіх розглянутих в роботі [6] варіантів, де фотомонтаж був побудований з зображеннями в різних (з/без втрат) форматах збереження).

Таблиця 1

Оцінка ефективності розробленого методу

Метод	Помилки 1-го роду (%)	Помилки 2-го роду (%)
Метод, запропонований в [6]	23	3
Розроблений метод	14	8

Як видно з наведених результатів, запропонований метод дещо поступається аналогу в сенсі помилок 2-го роду (хибних тривог), але значно перевершує в сенсі помилок 1-го роду – на 39%. Говорячи про основну мету роботи, треба зазначити, що в умовах проведення експертизи ключову роль відіграють саме помилки 1-го роду: критичним є пропуск фальсифікованого ЦЗ, тому зниження рівня саме цих помилок може розцінюватися як підвищення ефективності процесу саме виявлення результатів фотомонтажу.

Висновки. В роботі вирішена важлива науково-практична задача підвищення ефективності процесу виявлення порушення цілісності цифрового зображення шляхом розробки методу виявлення факту фотомонтажу. Метод розроблений на основі аналізу властивостей МНСЧ, множини X елементів МНСЧ, що мають максимальні значення, та околів елементів з множини X. Показники ефективності запропонованого методу становлять: 14 і 8% – помилки 1-го і 2-го роду відповідно, що дозволило підвищити ефективність виявлення результатів фотомонтажу на 39% (в сенсі помилок 1-го роду) в порівнянні з сучасним аналогом, що має аналогічну область застосування та схожий математичний базис (заснований на аналізі СНЧ блоків матриці ЦЗ).

В ході розробки метода виявлення фотомонтажу в ЦЗ:

- Досліджено властивості матриці найменших сингулярних чисел блоків, що ставиться у відповідність ЦЗ, для різних форматів (з втратами, без втрат) збереження, в результаті чого обґрунтовано і практично підтверджено:
  - значення елементів МНСЧ для ЦЗ в форматі з втратами в сукупності перевищують значення елементів МНСЧ для ЦЗ в форматі без втрат.
  - гістограми значень елементів МНСЧ для зображень без втрат не можуть мати моду, що перевищує 2; гістограми значень елементів МНСЧ для зображень з втратами не можуть мати моду, що дорівнює 0;
  - у випадку моди гістограми значень елементів МНСЧ 1 або 2, висновок про формат ЦЗ залежить від максимального значення МНСЧ.
- На основі встановлених властивостей МНСЧ розроблено метод відокремлення ЦЗ в різних форматах збереження: з втратами та без втрат.

Запропоновані в роботі методи мають незначну обчислювальну складність, яка для ЦЗ з $n \times n$-матрицею становить $O(n^2)$ операцій, оскільки визначається кількістю блоків, отриманих шляхом стандартної розбивки матриці ЦЗ.

Методи можуть бути застосовані для експертизи цілісності як ЦЗ, так і цифрового відео (при проведенні експертизи покадрово), а враховуючи їх поліноміальну ступеня 2 обчислювальну складність є перспективними при застосуванні навіть в режимі реального часу для цифрового відео.

Список літератури

1. Пирцхалава Л.Г. Хорошко В.О., Шелест М.Є., Хохлачьова Ю.Є.. Інформаційно-аналітичне забезпечення безпеки: монографія. Київ: ФЛП Ямчинський А.В., 2021. 470 с.
2. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. URL: https://tzi.ua/assets/files/1.1_003_99.pdf

3. Хорошко В.О., Павлов І.М., Бобало Ю.Я., Дудикевич В.Б., Опірський І.Р.,.Пархуць Л.Т. Проєктування комплексних систем захисту інформації. Львів: Видавництво Львівської політехніки, 2020. 320 с.
4. Siddiqi M.H., Asghar K., Draz U. Image Splicing-Based Forgery Detection Using Discrete Wavelet Transform and Edge Weighted Local Binary Patterns. *Security and Communication Networks*. 2021. V. 2021. 4270776. URL: https://doi.org/10.1155/2021/4270776
5. Hosny K. M., Mortda A.M., Lashin N.A., Fouda M.M. A New Method to Detect Splicing Image Forgery Using Convolutional Neural Network. *Appl. Sci.* 2023. V. 13(3). P.1272.
6. Зорило В.В. Метод підвищення ефективності виявлення порушення цілісності цифрового зображення: дис. канд. техн. наук: 05.13.21. К., 2013. 127 с.
7. Bi X., Zhang Z., Xiao B. Reality Transform Adversarial Generators for Image Splicing Forgery Detection and Localization. *Proceedings of the 2021 IEEE/CVF International Conference on Computer Vision (ICCV). Montreal, Canada*. 2021. P. 14294-14303.
8. Gonzalez R.C., Woods R.E. Digital Image Processing. 4th Ed. New York: Pearson, 2017. 1192 p.
9. Кобозєва А.А., Хорошко В.О. Аналіз інформаційної безпеки: монографія. К.: ДУІКТ, 2009. 251 с.
10. Bergman C., Davidson J. Unitary embedding for data hiding with the SVD. *Proceedings of SPIE – The International Society for Optical Engineering. Bellingham*. 2005. V. 5681, P. 619-630.
11. James W. Demmel. Applied Numerical Linear Algebra. Society for Industrial and Applied Mathematics, 1997. 419 p.

METHOD FOR IMAGE SPLICING FORGERY DETECTION

Kobozieva A.A.[1], Yenakiiev B.G.[2]

[1]Odesa I.I. Mechnikov National University,
2, Dvorianska St. , Odesa, 65082, Ukraine,
email: alla_kobozeva@ukr.net
[2]National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine
email: enakievb@gmail.com

The integrity of the information content, in particular the digital image considered in the work, is one of the criteria for its security. Image splicing is one of the most common methods of forgery today. This way of breaking the integrity of the image is easily implemented with the help of modern graphic editors (PhotoShop, Gimp, etc.). During image splicing, one image is created from several. The task of detecting image splicing is the subject of research by scientists in the field of information security around the world, but it remains relevant today: there are no universal expert methods that can even detect the presence of a "foreign" part in any case of image splicing; the effectiveness of existing methods needs to be increased even in limited conditions of their application. The paper presents a new polynomial degree 2 expert method, which makes it possible to separate the original image from one whose integrity is violated. The method is based on the analysis of the properties of the blocks smallest singular values matrix, which corresponds to the matrix of the digital image. The method localizes the area containing the part of another image. The developed method is based on established differences in the properties of the blocks smallest singular values matrix for digital images in different formats - lossy and lossless. These differences are reflected in the additional method of separating images in different formats proposed in the work. This method can be used both alone and as a component of the developed image splicing detection method in the case where the falsified image consists of parts of images stored with loss and without loss. It was established that the proposed expert method provides an increase in the efficiency of image splicing detection in comparison with the modern analogue method

Keywords: digital image, photomontage, singular number, matrix of the smallest singular values

DOI 10.15276/imms.v14.no1-2.37
УДК 519.6:004.93

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 37-44

РОЗРОБКА ТА ТЕСТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ВЕБ-ДОДАТКІВ

Ю.Ю. Козіна[1], Б.І. Юхименко[2], О.В. Іщенко[3]

Національний університет «Одеська політехніка»,
1, Шевченка пр., Одеса, 65044, Україна
emails: yuliyakc21@gmail.com[1], biruteyu@gmail.com[2], alesya.ishchenko@gmail.com[3]

В умовах росту інформаційних технологій все більшу популярність і потрібність набувають додатки, що розробляються для використання їх на різних платформах – кросплатформенні додатки. Це обумовлено появою та розвитком всіляких пристроїв, на яких вони можуть функціонувати. Одним з напрямків, що швидко розвиваються в галузі багатоплатформеності в даний час, є розробка додатків, що працюють на різних операційних системах, таких як десктопні – Windows, Mac OS, мобільні – iOS, Android. Однак, існуючі методики їх розробки орієнтовані на створення додатків під конкретну операційну систему, що обмежує універсальність їх застосування. У роботі вирішено актуальне завдання розробки та тестування інформаційної системи кросплатформних веб-додатків, використовуючи зв'язку фреймворків. Так само, в роботі проведено аналіз новітніх методик та інструментів кросплатформної розробки та їх засобів автоматизованого тестування. У підсумку розроблено багатоплатформний програмний продукт, який реалізує архітектуру «клієнт-сервер» та працює на платформах ios, android, і так само в будь-якому web браузері. Розроблений програмний продукт дозволяє користувачам зберігати та отримувати доступ до своїх нотатків на різноманітних платформах та редагувати їх.
Ключові слова*:* тестування, кросплатформні додатки, клієнт-серверна архітектура.

Вступ. Існуючі методики розробки кросплатформних веб-додатків орієнтовані на створення програмного забезпечення під конкретну операційну систему, що обмежує універсальність їх застосування. Наприклад, додатки, розроблені під систему Windows не завжди будуть працювати на мобільних платформах. А з урахуванням зростаючого попиту на мобільні додатки, актуальність вирішення даного протиріччя зростає. Крім того, досягнення високої якості розробки кросплатформних додатків може бути забезпечено ефективною організацією процесу їх автоматизованого тестування. Задача дослідження підходів до розробки кросплатформних веб-додатків з високим ступенем переносимості коду є актуальною на даний час. Крім того, треба шукати шляхи, які дозволять гнучке нарощувати функціонал для клієнт-серверних задач.

Мета роботи. Вимоги практики розробки кросплатформних додатків, що функціонують на десктопних і мобільних платформах, а також організація процесу їх автоматизованого тестування обґрунтовують актуальність даної роботи. Метою роботи є розробка та тестування кросплатформної інформаційної системи (ІС), архітектура якої дозволить гнучке нарощувати функціонал для клієнт-серверних задач.

Основна частина. Основними критеріями до обґрунтування вибору підходу до розробки, інструментів та методології програмування при реалізації кросплатформних додатків обрано: високий відсоток переносимості коду; продуктивність; безкоштовність продуктів; швидкість розробки; якість кінцевого продукту.

Виберемо підхід, що використовує фреймворки та зробимо вибір фреймворків кросплатформної розробки, який ґрунтується на відповідності сильних та слабких сторін фреймворків наведеним критеріям. Обрано Titanium SDK[1]. Він є безкоштовний. Має високу переносимість коду, поступається тільки PhoneGap за цим параметром, проте виграє у нього в продуктивності. Швидкості розробки сприяє велика

кількість готових рішень «з коробки». Однак якість продукту може постраждати через те, що використовувана мова javascript асинхронна та в численних розгалуженнях програмісту легко помилитися. Додатково розглянемо ще такий додатковий побічний критерій, як популярність та її динаміка використання, для цього скористаємося сервісом «Google trends» – рис. 1. По порівняння було обрано фреймворки: Titanium, PhoneGap та Xamarin.

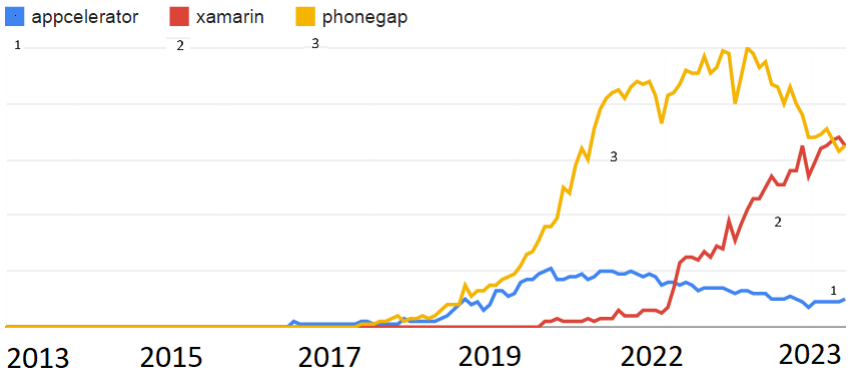


Рис. 1. Популярність та її динаміка використання фреймворків

Titanium SDK на графіку Google trends представляє «appcelerator» так як це ключове слово найбільш поширено для його пошуку. Як ми бачимо Titanium найменш популярний з розглянутих фреймворків, але його динаміка володіє деякою стабільністю. Це говорить нам про те, що ми стикаємося з проблемою слабкої підтримки фреймворку з боку співтовариства, але ми цілком можемо розраховувати, що цей фреймворк матиме підтримку з боку власника і не буде покинутий найближчим часом. Але так як нашим завданням є клієнт-серверне програмне забезпечення, то нам також потрібен інструментарій для створення серверної частини – веб-сервіс зі своїм API. Хоча Titanium SDK і дозволяє написання веб-додатків, але його функціонал призначений для самостійних додатків і написання веб-сервісу на ньому буде недоцільно. Тому виберемо потрібний інструментарій [2]. Результатом вибору буде – Node.js. Цей фреймворк повністю безкоштовний, виграє в продуктивності у аналогів за рахунок асинхронності. Швидкість розробки висока за рахунок декількох факторів:
– мова javascript. Одна мова для двох фреймворків дає незаперечний плюс в швидкості розробки, так як програмісту не потрібно буде переключатися з однієї мови на іншу;
– багата бібліотека готових рішень (модулів) npm і мінімум готових рішень у чистій збірці Node.js. Ці два фактори в комплексі дозволяють використовувати тільки ті модулі які потрібні і ніяких зайвих, це особливо корисно якщо враховувати, що нам потрібно створювати за допомогою цього інструменту не цілий веб-сайт, а тільки веб-сервіс і нам не потрібні всякі модулі та заготовки для веб-сайтів як у фреймворків конкурентів (не враховуючи Spring, він так само має високий рівень «модульності»).

При всіх перевагах, все ж таки залишається уразливість з якістю кінцевого продукту із за асинхронності як і у випадку з Titanium SDK. Для усунення вразливостей пов'язаних з помилками при написанні коду, будемо використовувати таку методологію програмування як BDD.

Розглянемо такі інструменти автоматизованого тестування, які одночасно працюють з Node.js і Titanium SDK:

1) Ti-mocha – це перенесена версія Mocha під Titanium SDK, іншого трохи менш популярного BDD фреймворка для javascript. На відміну від Jasmine, Mocha не має вбудованої бібліотеки тверджень і бібліотеки для роботи з заглушками, що швидше йде в плюс, тому що можна налаштувати його під себе. До нього можна

без проблем підключити такі бібліотеки як: should.js, assert.js, які дозволяють використовувати такі ключові слова як should (повинен) або як assert (очікується). А так само використовувати таку потужну бібліотеку для заглушок як Sinon. Ti mocha разом з бібліотекою тверджень should є головним претендентом для вибору як BDD фреймворку для Titanium.

2) Tishadow. Розробники цього продукту позиціонують його як повний набір інструментів для швидкої розробки додатків на Titanium SDK. Крім BDD фреймворку він включає в себе інструменти для швидкого розгортання додатків під всі платформи. BDD фреймворк заснований на реалізаціях Jasmine під Titanium і володіє всіма сильними і слабкими сторонами Jasmine. Але на відміну від Titanium-Jasmine цей проект постійно оновлюється.
3) Ticalabash – це перенесена версія фреймворку calabash для автоматизованого тестування для мобільних платформ. Calabash є ПЗ з відкритим вихідним кодом і широко використовується серед розробників. Основним плюсом calabash є те, що він використовує BDD фреймворк Cucumber, який дозволяє писати тести на мові максимально наближеної до природної мови. При всіх перевагах великою проблемою Ticalabash є його помилки і не стабільність.

Виходячи з аналізу розглянутих BDD фреймворків вибираємо Ti-mocha в зв'язці з should.js, і використовуємо таку ж зв'язку під Node.js.

Зауважимо що, так як ми використовуємо методологію розробки BDD, то специфікація додатка описується в тому ж стилі, що і тести, якби дублюючі їх. Так само слід розділяти поняття користувач і користувач програми. Під користувачем мається на увазі об'єкт в додатку, а користувач програми це людина яка використовує наше програмне забезпечення.

Перелічимо функціональні вимоги до системи:

1) Система повинна дозволяти, використовуючи зв'язку «пароль-ім'я користувача», створювати нового користувача.
2) Система повинна зберігати інформацію про користувача в базі даних.
3) Система повинна перевіряти при створенні користувача, що користувач додатки не помилився при введенні пароля, за допомогою підтвердження пароля, і повідомляти його в іншому випадку.
4) Система повинна дозволяти користувачеві додатки виконувати вхід в свій аккаунт допомогою правильно введеної комбінацією «пароль-ім'я користувача».
5) Система після входу користувача повинна відображати профіль користувача.
6) Система при повторному відкритті програми після його закриття повинна автоматично виконувати вхід, якщо це можливо, якщо ні, то пропонувати користувачеві додатки повторно ввести комбінацію «пароль-ім'я користувача».
7) Система повинна дозволяти користувачеві виконати вихід з усіх пристроїв.
8) Система повинна дозволяти користувачеві зберігати нотатки в своєму акаунті.
9) Система повинна дозволяти користувачеві видаляти та змінювати його нотатки.

Розглянемо нефункціональні вимоги.

Система повинна функціонувати на мобільних пристроях з ОС Android, Ios, а так само на інших платформах через web інтерфейс.

Всі дані системи повинні зберігатися в одному місці (на сервері).

Проектована інформаційна система буде створена на основі клієнт-серверної архітектури. Архітектура клієнт-сервер – обчислювальна або мережева архітектура, в якій завдання або мережева навантаження розподілені між постачальниками послуг, званими серверами, і замовниками послуг, званими клієнтами. Фізично клієнт і сервер – це програмне забезпечення. Зазвичай, вони взаємодіють через комп'ютерну мережу за допомогою мережевих протоколів і знаходяться на різних обчислювальних машинах. Сервера очікують від клієнтських програм запити і надають їм свої ресурси у вигляді даних. У нашому випадку роль сервера виконує додаток на Node.js, клієнти – додатки

що виконуються на різних платформах (мобільні та web) написані на Titanium SDK. Клієнти посилають запити на різні операції з об'єктом користувача або мікро повідомлень, сервер в свою чергу працює з базою даних і повертає потрібні дані клієнтам. Спілкування між клієнтами і сервером йде через протокол передачі гіпертексту HTTP (англ. HyperText Transfer Protocol).

Використовуються такі методи HTTP:

– OPTIONS. Надсилається клієнтами для отримання списку дозволених методів;
– GET. Використовується для отримання запитуваного вмісту;
– POST. Застосовується для передачі даних до серверу;
– DELETE. Запит на видалення якихось даних.

Використовуваний формат даних для передачі в обидві сторони – JSON.

Серверна частина це ядро всієї інформаційної системи. Практично весь функціонал реалізується на сервері, це і створення користувачів, і система аутентифікації, і система нотаток повідомлень, робота з базою даних. Для того щоб надати доступ до всіх цих функцій додаткам клієнтам, на сервері необхідно реалізувати механізм який буде розуміти HTTP запити клієнтів і повертати їм потрібні дані – REST API. У REST API в якості формату запитів до сервера використовується URI – аналог гіперпосилання в веб браузері. Сервер розпізнає URI і метод HTTP запиту і виконує відповідні дії, потім повертає дані клієнта. Для створення REST API сервера, ми будемо використовувати спеціально призначене розширення для Node.js під назвою Restify. Систему управління базою даних ми виберемо основну для більшості Node додатків – MongoDB, а так само розширення для Node для роботи з нею – Mongoose. Насамперед створимо структуру нашої бази даних. У нас є дві сутності: користувачі та нотатки. Користувач може мати багато нотаток, а нотатка тільки одного користувача. Для сутності користувача нам потрібні такі атрибути:

– Id. Первинний ключ;
– Username. Унікальне ім'я користувача;
– Password_hash. Хеш-сума пароля для аутентифікації;
– Token. Унікальний ключ використовується для аутентифікації.

Атрибути для сутності нотаток:

– Id;
– User_id. Зовнішній ключ для зв'язку з користувачем;
– Body. Текст нотатки;
– Title. Тема повідомлення;
– Created_at. Час створення повідомлення.

Схема бази даних в нотації UML зображена на рис. 2.

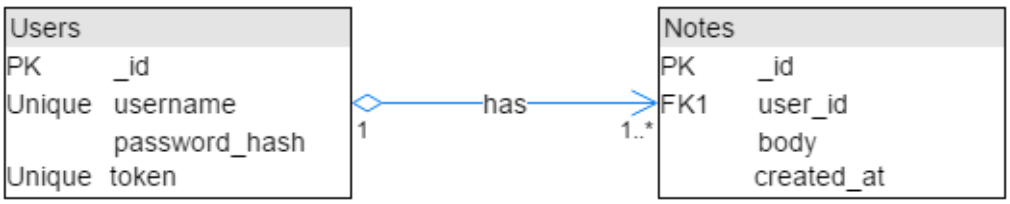


Рис.2. Схема БД в нотації UML

Наступним нашим кроком буде реалізація реєстрації (створення користувача). Для цього спочатку ініціалізуємо нашу базу даних і створимо модель користувача User (Додаток В), яка містить опис схеми моделі для її зв'язку з БД. Далі створимо в контролері користувача функцію «signup», яка відповідатиме за створення користувача. Функція «signup» отримує на вході такі аргументи: ім'я користувача; пароль.

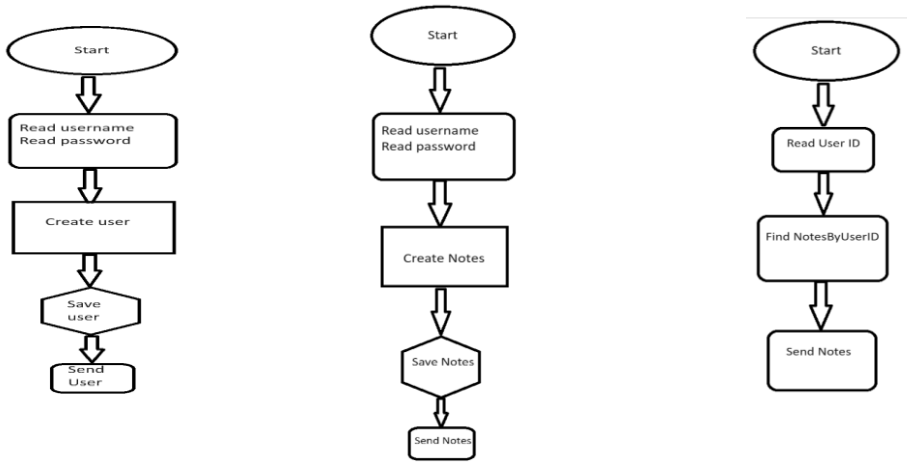
Далі функція обчислює хеш-суму пароля за допомогою алгоритму bcrypt [3], і генерує випадковий рядок, який буде використаний як секретний ключ при

аутентифікації. Далі функція створює модель з параметрами зазначеними вище, зберігає її в базу даних і повертає клієнту об'єкт користувача без поля з хеш-сумою пароля. Далі нам потрібно дати доступ до цієї функції клієнтам, для цього у файлі контролера маршрутів пропишемо маршрут POST HTTP запиту для URI: «/api/signup». Функція реєстрації на цьому закінчена. Блок схема даної функції зображена на рис 3a.
Наступним кроком буде реалізація системи аутентифікації. Для цього створимо функцію «signin» в контролері користувача. Вхідними аргументами цієї функції будуть ім'я користувача та пароль. Далі ми шукаємо відповідного користувача в базі даних і звіряємо хеш-суму пароля із запиту і хеш-суму пароля в базі даних, якщо вони збігаються, генеруємо новий секретний ключ в поле «token» і повертаємо об'єкт користувача клієнту, якщо ні, повертаємо користувачеві об'єкт з повідомленням про помилку. Прописуємо маршрут GET HTTP запиту для URI: «/api/signin».

Але кожен раз надсилати комбінацію «ім'я користувача-пароль» небезпечно і недоцільно, тому так само реалізуємо функцію аутентифікації по секретному ключу, який ми генерували раніше. Функція «signinByToken» повинна приймати на вході секретний ключ від клієнта, далі шукаємо його в базі даних і якщо він знайдений, повертаємо клієнту об'єкт користувача, якщо ні, повертаємо повідомлення про помилку. Прописуємо маршрут GET HTTP запиту для URI: «/api/user».

Останнім кроком системи аутентифікації буде реалізація функція виходу – logout. Функція записується за аналогією з попередніми функціями у файлі контролера користувача і виконує одну просту операцію, створює новий секретний ключ. Прописуємо маршрут GET HTTP запиту для URI: «/api/logout».

Далі реалізуємо систему нотаток, для цього створимо спочатку її модель. Потім створимо функції createNote і getNote і removeNote, які створюватимуть, отримуватимуть і видалятимуть нотатки. Доступ до цих функцій буде забезпечуватися через аутентифікацію по ключу доступу, тому в цих функціях об'єкт користувача буде завжди визначений. Функція createNote буде отримувати на вході текст нотатки. Далі функція буде створювати екземпляр моделі нотаток, і зберігати модель в БД. Блок схема даної функції зображена на рис3b.



a. b. c.

Рис. 3. Блок схеми функцій: «signup» (a), createNote (b), getNote (c)

Функція getNote отримує на вході id користувача і повертає клієнту всі пов'язані з поточним користувачем нотатки з БД. Блок схема даної функції зображена на рис.3c.

При розробці системи, нам требо генерувати унікальні ідентифікатори, які використовуються для аутентифікації користувачів.

Так як ідентифікатор, по суті, дає повний доступ до аккаунту користувача, до його генерації слід підійти серйозно, головна вимога до гарантії його унікальності, так як при співпаданні ідентифікаторів у різних користувачів, один з користувачів отримає

доступ до чужого аккаунту. Виходячи з цього ймовірність дворазового генерування одного і того ж ідентифікатора – виникнення колізії – повинна бути вкрай мала.

Так само ідентифікатор по можливості не повинен бути сильно довгим в цілях економії трафіку.

На ймовірність виникнення колізії впливають два фактори:

1) розмір ідентифікаційного простору – кількість можливих унікальних ідентифікаторів;

2) метод генерування ідентифікаторів – яким чином ідентифікатор вибирається із загального простору.

В ідеалі нам потрібно великий простір (щодо наших потреб), з якого випадково обираються рівномірно розподілені ідентифікатори. Тому для генерації випадкових рівномірно розподілених ідентифікаторів ми будемо конвертувати результат функції crypto.randomBytes(*N*), де *N* кількість повернених випадкових байт, у шістнадцятирічну строку. Ця функція, із пакету інструментів OpenSSL, є реалізацією криптографічно стійкого псевдовипадкового алгоритму який базується на «Вихрі Мерсена» [4]. Залишилося підрахувати скільки випадкових байт нас, влаштує, щоб ймовірність колізії була вкрай мала.

Представимо нашу задачу в наступному абстрактному вигляді: Дано n випадкових чисел з дискретного рівномірного розподілу з діапазоном $[1, H]$. Яка ймовірність $p(n, H)$, що, принаймні два числа збігаються?

Дана задача є узагальненням парадоксу днів народжень [5, 6]. Знайдемо зворотну ймовірність $\bar{p}(n, H)$ при $n < H$, таку що всі числа будуть різними:

$$\bar{p}(n, H) = 1 \times \left(1 - \frac{1}{H}\right) \times \left(1 - \frac{2}{H}\right) \times \ldots \times \left(1 - \frac{n-1}{H}\right). \quad (1)$$

Розкладання в ряд Тейлора експоненційної функції:

$$e^x = 1 + x + \frac{x^2}{2!} + \ldots \quad (2)$$

дає наближення першого порядку для x при $x \ll 1$:

$$e^x \approx 1 + x. \quad (3)$$

Щоб застосувати це наближення до формули (1) покладемо $x = -a / H$. Таким чином, отримаємо:

$$e^{-\frac{a}{H}} \approx 1 - \frac{a}{H} \quad (4)$$

Отримана апроксимація:

$$p(n, H) \approx 1 - e^{\frac{-n(n-1)}{2H}} \approx 1 - \left(\frac{H-1)}{H}\right)^{\frac{n(n-1)}{2}}. \quad (5)$$

Тепер напишемо формулу для оберненої задачі:

$$n(p,H) \approx \sqrt{2H \times \ln\left(\frac{1}{1-p}\right)}. \quad (6)$$

Якщо повернуться до задачі ймовірності виникнення колізій ідентифікаторів, то H – буде позначати розмір ідентифікаційного простору, p –ймовірність колізії, n – кількість згенерованих ідентифікаторів. Розмір ідентифікаційного простору обчислюється таким чином:

$$H = 2^{8N}, \quad (7)$$

де N – довжина ідентифікатора в байтах.

Використовуючи формули (5) і (6), складемо таблицю ймовірностей колізій для визначення потрібної довжини ідентифікатора. Нижче наведено фрагмент цієї таблиці:

Таблиця 1

Таблиця ймовірностей колізій

N	$p(n,H)$		Розрахунок років			
	1E-12	0,10%	$Y_1(10^{-12})$	$Y_2(10^{-12})$	$Y_1(0.1\%)$	$Y_2(0.1\%)$
2	< 2	8	--	--	--	--
4	< 2	2073	--	--	--	--
8	4295	1,36E+08	1E-07	8E-03	0,004	258
12	2,81E+08	8,90E+12	9E-03	536	282,320	2E+07
18	4,72E+15	1,49E+20	149752	9E+09	5E+09	3E+14
22	3,09E+20	9,79E+24	1E+10	6E+14	3E+14	2E+19

Де, Y_1 – кількість років для досягнення заданої ймовірності колізії при тисячі генераціях в секунду (реальний проект), Y_2 – кількість років для досягнення заданої ймовірності колізії при однієї генерації в хвилину (навчальний проект).

Виходячи з перерахованих даних, для навчального проекту можна прийняти довжину ідентифікатора рівну 8 байтам, що гарантує, що за 258 років, ми досягнемо ймовірності колізії в 0,1%. Для реального проекту варто вибрати > 12 байт.

Відсоток переносимого коду обчислювався таким способом:

$$\textbf{ВПК} = \frac{\text{кількість рядків переносимого коду}}{\text{загальна кількість рядків коду}} \cdot 100\% = \frac{323}{341} \cdot 100\% = 94.7\% \quad (8)$$

Відсоток покриття коду тестами обчислювався таким способом:

$$\textbf{ВПКТ} = \frac{\text{кількість рядків коду покритих тестами}}{\text{загальна кількість рядків коду}} \cdot 100\% = \frac{307}{341} \cdot 100\% = 90\% \quad (9)$$

$$\frac{307}{341} \cdot 100\% = 90\%.$$

Висновки. Рооозв’язане актуальне завдання розробки та тестування інформаційної системи кросплатформних веб-додатків, використовуючи зв'язку фреймворків. Так само в роботі проведено аналіз новітніх методик та інструментів кросплатформної розробки та їх засобів автоматизованого тестування.

У підсумку розроблено багатоплатформний програмний продукт, який реалізує архітектуру «клієнт-сервер» та працює на платформах ios, android, і так само в будь-якому web браузері. Розроблений програмний продукт дозволяє користувачам зберігати та отримувати доступ до своїх нотатків на різноманітних платформах та редагувати їх.

При цьому досягнуто відсоток переносимості коду в 94.7%, що є відмінним результатом. Якби ми писали код окремо під 3 кожні платформи, то було б імовірно в 2,84 рази більше рядків коду, звідси час, витрачений на розробку, за рахунок використання цієї зв'язки фреймворків та архітектури, було скорочено в 2,84 рази.

Список літератури

1. Titanium Platform Overview. URL: https://titaniumsdk.com/guide/ Titanium_SDK/Titanium_SDK_Getting_Started/ Titanium_Platform_Overview.html
2. Spring Framework Advantages and Disadvantages. URL: http://www.aksindiblog.com/spring-framework-advantages-disadvantages.html
3. Bcrypt. URL: https://en.wikipedia.org/wiki/Bcrypt
4. Mersenne Twister Home Page. URL: http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html
5. Birthday problem . URL: https://en.wikipedia.org/wiki/Birthday_problem
6. Lundy M., Mees A. Convergence of an annealing algorithm. *Math. Programing.* 1996. V.34. P.111-124. URL: https://link.springer.com/article/10.1007/BF01582166

DEVELOPMENT AND TESTING OF WEB APPLICATIONS INFORMATION SYSTEM

Yu.Yu. Kozina[1], B.I. Yukhimenko[2], O.V. Ischenko[3]

National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine
emails: yuliyakc21@gmail.com[1], biruteyu@gmail.com2, alesya.ishchenko@gmail.com[3]

In the conditions of the growth of information technologies, applications developed for usage on the different platforms – cross-platform applications – are gaining more and more popularity and need. This is due to the appearance and development of all kinds of devices on which they can function. One of the rapidly developing directions in the field of multi-platform is currently the development of applications that work on different operating systems, such as desktop – Windows, Mac OS, mobile – iOS, Android. However, the existing methods of their development are focused on creating applications for a specific operating system, which limits the universality of their application. The work solves the urgent task of developing and testing the information system of cross-platform web applications using the framework connection. Also, the work analyzes the latest methods and tools of cross-platform development and their means of automated testing. As a result, a multi-platform software product was developed, which implements the "client-server" architecture and works on the ios, android platforms, as well as in any web browser. The software product developed allows users to save and access their notes on various platforms and edit them.

Keywords: Testing, cross-platform applications, client-server architecture.

DOI 10.15276/imms.v14.no1-2.45
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 45-55

РОЗРОБКА ПЛАГІНУ ДЛЯ ПРОГРАМИ BLENDER З МЕТОЮ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В 3D МОДЕЛЮВАННІ

А.В. Лозовський, Н.І. Кушніренко, В.О. Назаров, В.В. Подуфалов

Національний університет «Одеська Політехніка»,
1, Шевченка пр., Одеса, 65044, Україна;
email: infsec2011@gmail.com

Робота присвячена аналізу питань, пов'язаних із захистом прав інтелектуальної власності на тривимірні моделі. У сучасному світі 3D-моделювання набуло широкого поширення та застосування в різних галузях, включаючи кіноіндустрію, відеоігри, медицину, архітектуру та виробництво. Швидкий розвиток технологій 3D-друку та цифрових платформ створює нові можливості, але водночас і нові виклики для правовласників. Однією з ключових проблем є поширення незаконного копіювання та використання 3D-моделей, що може призвести до значних фінансових втрат для авторів та компаній, які інвестують у розробку таких моделей. Традиційні правові механізми захисту, такі як авторське право, патенти та товарні знаки, не завжди ефективно працюють у контексті цифрового середовища, де порушення прав може відбуватися миттєво і в глобальному масштабі. У статті розглядаються різні підходи до захисту інтелектуальної власності на 3D-моделі. Зокрема, аналізуються можливості використання цифрових водяних знаків, криптографічних методів та інших технологічних засобів для забезпечення захисту від незаконного копіювання та розповсюдження. Результатом роботи є розроблений плагін для програми Blender, який забезпечує автоматичний захист авторських прав на кінцеві зображення за допомогою накладання цифрових водяних знаків. За допомогою розробленого плагіну автор може непомітно додати свій унікальний код у кінцеве зображення. Також користувач має можливість перевірити авторство завантаженого зображення. Розроблене рішення може знайти широке застосування серед творчих професіоналів.
Ключові слова: захист 3D проектів, цифрові водяні знаки, плагін, інтелектуальна власність, захист авторських прав.

Вступ. Сьогодні, коли технологічні інструменти стають більш доступними та потужними, а цифрові платформи здатні передавати та обробляти складні дані, захист інтелектуальної власності стає особливо важливим. Особливо це стосується галузей, де творчість і технології переплітаються, наприклад, 3D-моделювання.

Це питання особливо актуальне в контексті широкого використання 3D-моделей у відеоіграх, кіноіндустрії, медицині, архітектурному проектуванні та інших сферах. Велика кількість різноманітних об’єктів, які можна створювати та використовувати в цих галузях, створює потенційні можливості для порушення прав інтелектуальної власності [1]. Наприклад, для створення віртуальних світів у відеоіграх або реалістичних сцен у фільмах може знадобитися використання різних моделей і текстур, які можуть бути об’єктами авторського права. У медичній сфері, наприклад, розробка та використання 3D моделей дозволяє точніше планувати операції та лікування, але водночас потребує надійного захисту від несанкціонованого доступу. Архітектори та інженери використовують 3D моделі для візуалізації проектів та уточнення дизайну, але при цьому стикаються з ризиком порушення конфіденційності та крадіжки інтелектуальної власності [1, 2].

Крім того, зі зростанням популярності 3D-друку – методу створення 3D-моделей, зростає ризик незаконного використання чужих творінь у власних цілях. Такі ситуації можуть призвести до серйозних конфліктів між творцями та користувачами, а також до значних втрат, наприклад, фінансових [2].

Невідповідальне ставлення до захисту 3D проектів та інтелектуальної власності може мати серйозні наслідки для галузей, в яких активно використовуються 3D моделі, та для суспільства в цілому. Крім фінансових втрат для компаній і авторів, порушення прав на інтелектуальну власність може призвести до втрати довіри споживачів та зниження конкурентоспроможності на ринку [3]. Без ефективного захисту, потенційні досягнення та переваги від використання 3D технологій можуть бути втрачені.

Розуміння та вирішення проблем захисту інтелектуальної власності в 3D-моделюванні стає надзвичайно важливим завданням для подальшого розвитку цієї галузі. Використання новітніх технологій і розробка спеціалізованих інструментів, таких як плагіни, можуть стати важливими кроками в забезпеченні ефективного правового захисту та сприянні творчості у сфері 3D-моделювання [1].

У цьому контексті розробка плагіна для захисту інтелектуальної власності в 3D-моделюванні стає важливим кроком у забезпеченні безпеки та юридичної прозорості для творців і власників контенту. Плагін на основі стеганографічних алгоритмів може приховувати інформацію про авторські права та вбудовувати її безпосередньо в модель, роблячи її невидимою для неавторизованих користувачів, але легко доступною для правовласника.

Мета і задачі дослідження. Мета роботи полягає в підвищенні рівня захищеності 3D проектів шляхом розробки плагіна для програми Blender, який забезпечує автоматичний захист авторських прав на кінцеві зображення за допомогою накладання цифрових водяних знаків. Для досягнення цієї мети необхідно виконати наступні задачі:

1. Провести аналіз сучасного стану питання захисту 3D проектів, включаючи вразливості систем та потенційні загрози для інтелектуальної власності.

2. Дослідити різноманітні підходи до захисту інтелектуальної власності, включаючи шифрування даних, контроль доступу, водяні знаки та інші методи, а також оцінити їх ефективність та придатність для застосування в галузі 3D моделювання.

3. Розробити програмний продукт, який забезпечує захист інтелектуальної власності в контексті 3D проектів.

Виконання цих задач дозволить досягти поставленої мети підвищення рівня захищеності 3D проектів і забезпечити надійний захист інтелектуальної власності у цифровому середовищі.

Основна частина. Захист інтелектуальної власності в 3D-моделюванні стає все більш актуальним у сучасному світі. В основному це пов'язано з тим, що технології 3D-моделювання стають все більш доступними і потужними. Однак із цим покращенням доступності ризик порушення [2] прав інтелектуальної власності, природно, також зростає. Незахищені проекти стають дієвими мішенями для кіберзлочинців, які можуть їх викрасти або використати для підробок та інших шахрайських дій

Розглянемо більш детально загрози інформаційної безпеки для 3D проектів.

- Видалення або пошкодження даних: Зловмисники можуть здійснювати атаки з метою видалення чи пошкодження 3D моделей чи інших даних проекту. Це може призвести до втрати важливої інформації або навіть неможливості використання проекту.

- Зміна даних: Іншою загрозою є можливість несанкціонованої зміни даних у 3D проекті. Зловмисники можуть внести зміни, які призведуть до порушення цілісності проекту або навіть втрати його цінності.

- Втрата контроля над проектом: Якщо зловмисники отримають доступ до проекту і впровадять зміни або видаляють дані, це може призвести до втрати контролю над проектом та його подальшого використання [3, 4].

- Фінансові втрати: Негативний вплив на проект також може мати фінансові наслідки. Наприклад, якщо проект стає непридатним через атаки з боку зловмисників, це може призвести до втрати інвестицій або навіть до фінансових збитків.

- Порушення авторських прав в сфері 3D проектів може мати серйозні наслідки для творців інтелектуальної власності та їх проектів. Ось деякі з основних аспектів порушення авторських прав:

1) Несанкціоноване копіювання та використання: Зловмисники можуть копіювати та використовувати 3D проекти без дозволу їхніх авторів, що призводить до порушення авторських прав. Це може стати причиною фінансових втрат для творців та зниження їхнього контролю над власною творчістю.
2) Недозволене використання в комерційних цілях: Іншою загрозою є неприпустиме використання 3D проектів у комерційних цілях без згоди авторів. Це може призвести до втрати прибутку та порушення прав власності.
3) Втрата конфіденційності: Якщо 3D проекти стають доступними для несанкціонованого використання, це може призвести до втрати конфіденційної інформації або секретів, які можуть бути включені в проект..
4) Підробка та зміна авторства: Зловмисники можуть намагатися підробити авторство 3D проектів або змінити авторську інформацію для власних цілей. Це може призвести до плутанини щодо справжнього автора та порушення його прав [4].

- Соціальна інженерія є одним з найбільш вразливих аспектів безпеки у сфері 3D проектів. Це метод атаки, при якому зловмисник використовує маніпуляцію людьми з метою отримання конфіденційної інформації або доступу до системи. Деякі з прикладів атак, які використовують соціальну інженерію у сфері 3D проектів, включають:

1) Фішингові атаки: Зловмисники можуть використовувати фішингові електронні листи або повідомлення для отримання конфіденційної інформації від користувачів, такої як паролі або доступ до облікових записів, що може призвести до несанкціонованого доступу до 3D проектів.
2) Соціальні інженери: Зловмисники можуть намагатися встановити довіру з користувачем, щоб отримати доступ до його проектів або конфіденційної інформації.

Для захисту від соціальної інженерії важливо навчати користувачів розпізнавати підозрілі ситуації та надавати їм інструменти та інформацію про безпеку та захист даних. Також важливо використовувати технічні засоби захисту, такі як двофакторна аутентифікація та обмеження доступу до конфіденційної інформації.

Заходи захисту відповідають на загрози та вразливості, що існують у сфері 3D проектів. Нижче наведено деякі ключові заходи захисту, які можуть бути використані для забезпечення безпеки та захисту цих проектів:

- Використання шифрування даних забезпечує конфіденційність та цілісність інформації, що передається або зберігається у системі. Застосування шифрування дозволяє захистити 3D проекти від несанкціонованого доступу та перегляду.

- Контроль доступу: Встановлення багаторівневого контролю доступу дозволяє обмежити доступ до 3D проектів лише авторизованим користувачам. Це запобігає несанкціонованому використанню або редагуванню даних.

- Використання водяних знаків та електронних підписів [4, 5] допомагає підтвердити автентичність та походження 3D моделей та проектів, а також захистити їх від незаконного копіювання чи внесення змін.

- Резервне копіювання даних дозволяє запобігти втраті інформації в разі виявлення атаки або випадкового видалення файлів.

- Освіта та навчання користувачів щодо безпеки в Інтернеті, розпізнавання загроз та правил безпеки є важливим кроком для запобігання соціальній інженерії та інших видів атак.

- Проведення регулярного аудиту системи безпеки дозволяє виявляти потенційні вразливості та ризики, що можуть бути використані зловмисниками для атак.

- Встановлення та підтримка актуального антивірусного та антишпигунського програмного забезпечення допомагає виявляти та блокувати шкідливі програми та загрози для безпеки.

Застосування цих заходів захисту допомагає забезпечити надійний та ефективний захист 3D проектів від потенційних загроз та атак, зберігаючи конфіденційність та цілісність даних.

Розглянемо більш детально питання захисту інтелектуальної власності та авторських прав, як складової. На сьогоднішній день існує безліч методів та технік захисту інтелектуальної власності, спрямованих на попередження незаконного використання та копіювання контенту. При розгляді захисту інтелектуальної власності у галузі 3D моделювання важливо розуміти і вивчати існуючі підходи та їхні переваги та недоліки.

Одним із найпоширеніших підходів до захисту інтелектуальної власності є використання технологій DRM (Digital Rights Management). DRM – це набір технологій, який дозволяє обмежувати доступ до цифрового контенту та контролювати його використання шляхом застосування різних захисних механізмів, таких як шифрування, цифрові підписи та управління правами доступу [3].

Переваги DRM:

- Захист інтелектуальної власності: DRM допомагає запобігти несанкціонованому копіюванню, розповсюдженню та використанню цифрового вмісту, забезпечуючи компенсацію авторам і правовласникам за їхню роботу.

- Гарантія доходу: Обмежуючи неавторизований доступ, DRM гарантує, що лише клієнти, які платять, зможуть отримати доступ до вмісту, таким чином максимізуючи дохід для творців і розповсюджувачів вмісту.

- Контроль над використанням контенту: DRM дозволяє правовласникам контролювати, як їхній вміст використовується, розповсюджується та ділиться. Вони можуть установлювати обмеження на копіювання, друк і спільний доступ.

- Запобігання піратству: DRM є ефективним інструментом боротьби з цифровим піратством, яке може суттєво вплинути на доходи та сталість таких галузей, як музика, кіно, програмне забезпечення та видавництво.

- Покращена безпека: Технології DRM часто включають шифрування та безпечні методи автентифікації, які підвищують загальну безпеку цифрового контенту.

Однак, деякі експерти вважають, що DRM може бути неефективним у деяких випадках і навіть призводити до обмежень для законних користувачів [2].

Серед недоліків DRM слід виділити:

- Незручності для користувачів: DRM може ускладнити доступ законних користувачів до вільного використання вмісту, що призводить до розчарування та незадоволення. Обмеження на копіювання, спільний доступ і сумісність пристроїв можуть бути громіздкими.

- Проблеми сумісності: Вміст, захищений DRM, може бути несумісним з усіма пристроями та платформами, що обмежує можливість користувачів отримати доступ до придбаного вмісту на різних пристроях.

- Питання конфіденційності: Деякі системи DRM відстежують поведінку користувачів і шаблони використання, що викликає занепокоєння щодо конфіденційності серед споживачів, які цінують свою цифрову конфіденційність.

- Високі витрати: Впровадження та підтримка систем DRM може бути дорогим для творців і розповсюджувачів контенту. Ці витрати можуть бути перекладені на споживачів у вигляді вищих цін.

- Обмежене добросовісне використання: DRM може обмежувати можливість користувачів брати участь у діях добросовісного використання, таких як створення резервних копій, створення похідних робіт або використання вмісту в освітніх цілях.

- Можливість зловживання: Правовласники можуть зловживати надто обмежувальним режимом DRM для здійснення надмірного контролю над вмістом, пригнічуючи інновації та обмежуючи свободу користувачів використовувати вміст, який вони придбали законним шляхом.

Хоча DRM пропонує значні переваги з точки зору захисту інтелектуальної власності та забезпечення прибутку, він також створює проблеми, пов’язані зі зручністю для користувачів, сумісністю та конфіденційністю.

Поширеним підходом є індивідуальне використання водяних знаків (watermarks) [4] для захисту авторських прав. Водяні знаки є невидимими або малопомітними образами або текстом, які вбудовуються безпосередньо у контент. Вони дозволяють ідентифікувати автора чи власника контенту та встановлювати його права, а також служити попередженням для потенційних порушників. Однак, водяні знаки також можуть бути видалені або змінені недобросовісними користувачами, що зменшує їхню ефективність. Також, вони можуть впливати на якість візуального сприйняття моделі. Крім того, існують технології стеганографії, які дозволяють приховувати інформацію безпосередньо у цифрових файлах, зокрема, у 3D моделях. Ці технології дозволяють вбудовувати інформацію про авторство та власність без зміни зовнішнього вигляду моделі. Стеганографічні методи захисту можуть бути відносно ефективними, оскільки ускладнюють виявлення та видалення захисної інформації без відома автора.

Криптографія є одним із ключових інструментів для захисту авторських прав у цифровому середовищі. Застосування криптографічних методів дозволяє забезпечити конфіденційність, цілісність та автентичність інформації, що важливо для захисту творів інтелектуальної власності [5]. Нижче наведені основні способи використання криптографії для захисту авторських прав:

- Шифрування файлів: Використання шифрування для захисту цифрових файлів (музики, відео, програмного забезпечення, електронних книг) від несанкціонованого доступу та копіювання.
- Шифрування під час передачі: Шифрування даних під час їх передачі через мережу (наприклад, HTTPS для веб-сайтів), що запобігає їх перехопленню та несанкціонованому використанню.
- Аутентифікація авторства: Цифрові підписи забезпечують підтвердження авторства та цілісності твору, що допомагає запобігти його підробці та несанкціонованому використанню.
- Захист документів: Використання цифрових підписів для захисту важливих документів, таких як контракти, угоди про авторські права, забезпечує їх юридичну силу та захист від модифікацій.

Розглядаючи застосування водяних знаків та шифрування до 3D моделей, приходимо до наступних висновків:

- Водяні знаки можуть бути особливо корисними для ідентифікації авторства [1, 4] та власності у випадку об'ємних та складних 3D моделей, де вони можуть бути менш помітними для користувачів, аніж у двомірних зображеннях.
- Шифрування може бути ефективним для захисту конфіденційної інформації та комерційних секретів у випадку, коли доступ до моделі має бути у обмеженого кола осіб.

Враховуючи особливості кожного методу та їх застосування до 3D моделей, оптимальне рішення може полягати в комбінації цих методів для досягнення максимального рівня захисту інтелектуальної власності у галузі 3D моделювання.

Наступним важливим аспектом є правовий захист інтелектуальної власності, що включає в себе авторські права, патенти та інші юридичні механізми. Ці механізми дозволяють власникам захищати свої права на контент та відстежувати порушення через судову систему.

Захист інтелектуальної власності у сфері 3D моделювання має свої власні особливості та складності, які важливо враховувати при розробці та впровадженні методів захисту. Розглянемо деякі з них.

1. Складність структури 3D моделей: 3D моделі можуть бути дуже складними та містити велику кількість деталей, шарів та компонентів. Це може ускладнювати процес захисту, оскільки потрібно забезпечити захист для кожного елементу моделі.

2. Ризик інформаційних втрат [2] під час обміну даними: Передача 3D моделей між користувачами або учасниками проекту може призвести до ризику втрати конфіденційної інформації. Недобросовісні користувачі можуть намагатися витіснити чи використати моделі без дозволу власника.

3. Необхідність збереження якості та продуктивності: При застосуванні методів захисту до 3D моделей важливо зберігати якість та продуктивність моделі. Деякі методи захисту можуть впливати на продуктивність програм та процесів, пов'язаних зі створенням та редагуванням моделей.

4. Потреба у спеціалізованому програмному забезпеченні: Для ефективного захисту 3D моделей може знадобитися використання спеціалізованого програмного забезпечення, яке може бути дорогим або складним у використанні.

Враховуючи ці особливості та складності, важливо розробляти та впроваджувати методи захисту, які забезпечують ефективний рівень захисту, при цьому не погіршуючи продуктивність та якість 3D моделей. Крім того, необхідно враховувати потреби та очікування користувачів у плані зручності та ефективності використання захисних методів.

Плагін для захисту авторських прав у 3D проектах в пакеті Blender. Для розробки 3D проектів, а також реалізації їх захисту важливо обрати потужні та надійні інструменти та програмне забезпечення. На ринку існує багато програм для створення 3D моделей та проектів, серед яких можна виділити такі відомі програми як Autodesk Maya, 3ds Max, Cinema 4D, SolidWorks та Blender.

Autodesk Maya та 3ds Max є досить популярними програмами, які широко використовуються у сфері 3D моделювання та анімації. Вони мають розширений набір інструментів і можливостей, але вимагають певного часу для вивчення та експлуатації.

Cinema 4D також відомий своєю простотою використання та інтуїтивним інтерфейсом, що робить його популярним серед початківців у сфері 3D.

SolidWorks використовується переважно для промислового дизайну та інженерії, але також має інструменти для створення 3D моделей.

Однак, серед усіх цих програм можна виділити Blender. Blender є безкоштовним та відкритим програмним забезпеченням з потужним функціоналом для створення 3D моделей, анімації та рендерингу. Він підтримує всі необхідні функції для реалізації проектів у сфері 3D, включаючи моделювання, текстування, анімацію, композитинг та багато іншого.

Ось декілька переваг Blender [6], які роблять його найкращим вибором для реалізації захисту проектів у сфері 3D:

1. Відкритий код: Blender є безкоштовним та має відкритий вихідний код, що дозволяє розробникам та користувачам перевіряти, адаптувати та вдосконалювати програму з метою забезпечення безпеки.

2. Активна спільнота: Blender має велику активне ком’юніті користувачів та розробників, яка постійно вносить покращення та забезпечує підтримку.

3. Широкі можливості: Blender має широкий набір інструментів для реалізації різноманітних проектів у сфері 3D, що дозволяє створювати складні та захищені моделі.

4. Підтримка різних платформ: Blender підтримує різні операційні системи, що робить його доступним для широкого кола користувачів.

Узагальнюючи, Blender є найкращим вибором для реалізації захисту проектів у сфері 3D завдяки своїй потужній функціональності, відсутності плати за використання

та відкритості вихідного коду, активній спільноті та широким можливостям [7]. Саме на основі цього програмного забезпечення розроблено плагін для захисту авторських прав, запропонований а даній роботі.

У даній роботі пропонується нове розширення для програмного забезпечення Blender. Плагін надає можливість для реєстрації та авторизації користувача. Після чого користувачу присвоюється індивідуальний код. Під час рендеру цей унікальний код непомітно вбудовується у кінцеве зображення за допомогою методу Коха і Жао [8].

Ця розробка також може працювати й у зворотному напрямку. Після авторизації виконавець має можливість дізнатися, чи належить йому авторство того чи іншого завантаженого зображення. Після встановлення розширення в 3D Viewport з'являться нова вкладка Render in safety, в якій стає доступним інтерфейс реєстрації (рис. 1).

Рис.1. Інтерфейс плагіна до авторизації

На початковому екрані з'являється панель реєстрації та авторизації. Дані користувача зберігаються на сервері, тому один акаунт можна зареєструватися лише раз, код прив'язаний лише до однієї пошти й не може збігатися з іншими номерами, тобто він однозначно ідентифікує користувача.

У плагіна є вимоги до паролю, якщо пароль користувача їм не відповідає, то з'являється відповідне повідомлення, яке інформує, що щось не так. Також є і інші повідомлення про помилки, наприклад, для таких випадків: невірні дані для логіна, відсутність імейла в системі і тому подібне (рис. 2).

Приклад повідомлення про помилку:

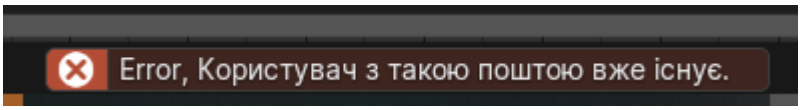


Рис.2. Демонстрація помилки

Спочатку користувачу необхідно зареєструватися, ввівши свою пошту та пароль. Після цього на цю пошту прийде лист з підтвердженням. Після підтвердження з'явиться можливість увійти в обліковій запис і вільно користуватися ним.

Після авторизації з'являться функціонал, наведений на рисунку 3.

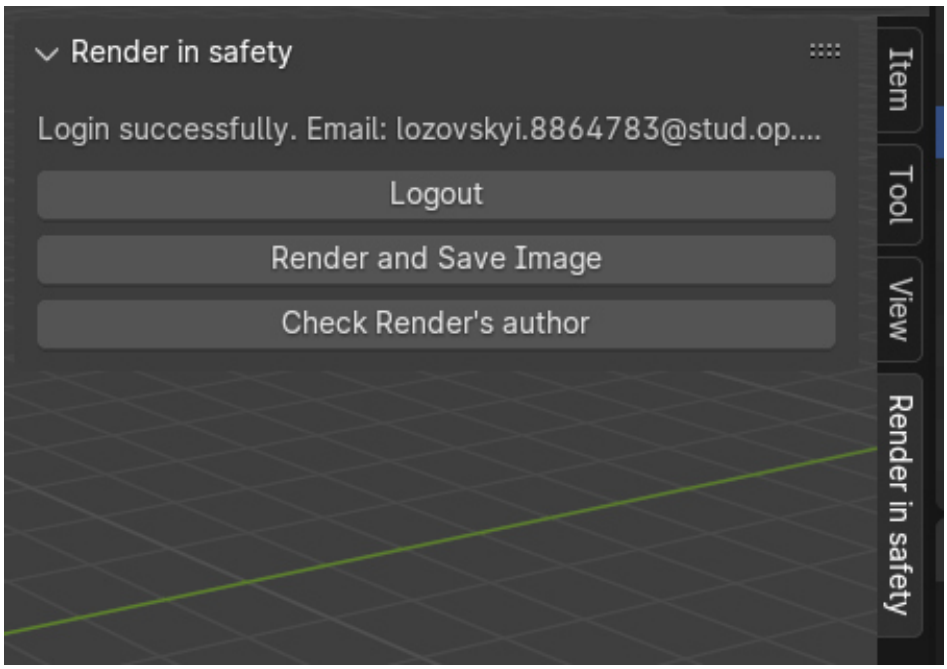


Рис.3. Інтерфейс плагіна після авторизації

Тепер виникла можливість вийти з акаунта, зробити рендер з вбудованим в зображення унікального коду користувача за алгоритмом Коха і Жао та перевірити зображення на збіг коду. Якщо натиснути на Render and Save Image, з'явиться інтерфейс збереження рендеру з назвою за замовчування render.png та можливістю обрати шлях для збереження кінцевого зображення. Після використання плагіна, в робочому просторі буде існувати 2 файли: default – звичайний рендер, render – рендер з вбудовуванням індивідуального коду за допомогою плагіна (рис. 4).

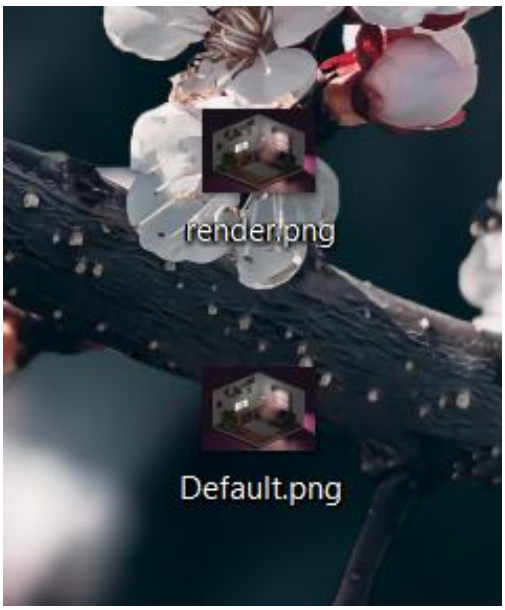


Рис.4. Збережені файли

Через те, що вбудовування інформації в зображення за допомогою алгоритму Коха і Жао абсолютно непомітне неозброєним оком, ми можемо бути впевнені, що різниця між зображеннями відсутня (рис. 5 а та б).

а) звичайне зображення б) зображення з вбудовуванням

Рис. 5. Порівняння звичайного та модифікованого зображення

Далі, за допомогою функціоналу Check render author, перевіримо зображення render.png на авторство (рис. 6). Під час перевірки зображення файлу render.png, плагін видав повідомлення, що «Я автор цього зображення» (рис. 7), а для іншого зображення – ні, бо в нього код власника не вбудовувався.

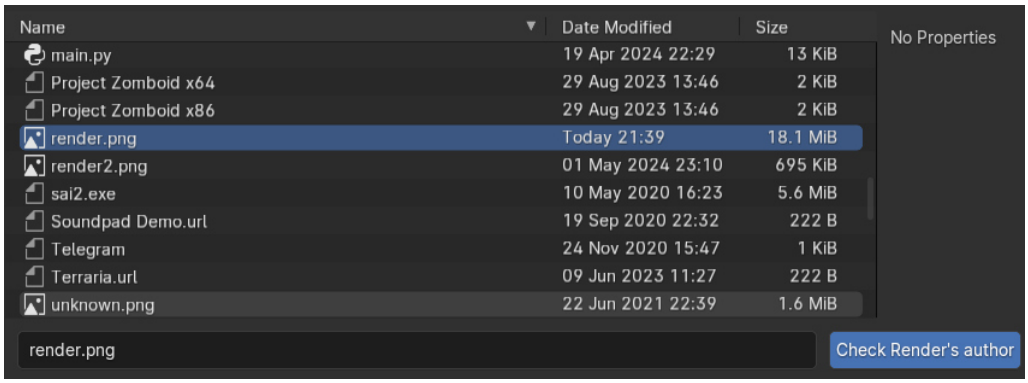


Рис. 6. Перевірка зображення на авторство

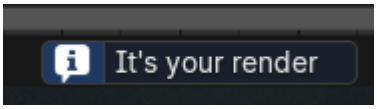


Рис. 7. Повідомлення плагіна, яке підтверджує авторство

Розроблений плагін реалізує кілька важливих функцій, спрямованих на збереження права власності виконавців та запобігання незаконному використанню їхніх робіт, серед яких:

1. Захист права власності виконавця. Однією з ключових функцій є забезпечення надійного захисту авторських прав на зображення, створені в Blender. Плагін дозволяє виконавцям вбудовувати невидимі водяні знаки у свої роботи, які важко видалити або змінити без значного погіршення якості зображення. Це забезпечує впевненість у тому, що права на створені зображення будуть збережені, навіть якщо вони поширюються через Інтернет або інші цифрові канали
2. Інтеграція з Blender. Плагін розроблений для безшовної інтеграції з Blender, що дозволяє користувачам легко використовувати його функції без необхідності переходу на інше програмне забезпечення. Це знижує бар'єри для впровадження технології захисту авторських прав та забезпечує ширше використання плагіна серед творчих професіоналів.

3. Використання методу Коха і Жао. Плагін використовує метод Коха і Жао для вбудовування унікальних кодів у зображення. Цей метод є одним з найбільш ефективних для створення стійких водяних знаків, які витримують різні типи обробки зображень, включаючи стиснення, фільтрацію та зміну формату. Водяні знаки, створені за цим методом, залишаються невидимими для людського ока, але можуть бути легко розпізнані спеціальними алгоритмами, що забезпечує надійний захист авторських прав.

4. Універсальність. Плагін розроблений для роботи в обох напрямках – як для захисту нових зображень, так і для перевірки авторства існуючих. Це дозволяє користувачам не лише захищати свої роботи, але й перевіряти, чи їхні роботи не були незаконно використані іншими особами. Користувач може завантажити будь-яке зображення, і система визначить, чи є воно захищеним, і хто є його автором. Це особливо корисно для виконавців, які хочуть перевірити, чи не були їхні зображення використані без дозволу.

5. Простота використання: Одним з важливих аспектів розробки є створення зручного та інтуїтивно зрозумілого інтерфейсу користувача. Це забезпечує легкість реєстрації, авторизації та використання функцій плагіна без необхідності глибоких технічних знань. Інтерфейс дозволяє користувачам швидко отримати доступ до всіх необхідних функцій та інструментів для захисту їхніх робіт.

Висновки. Розглянуто проблему захисту інтелектуальної власності у контексті 3D моделювання. Проведено аналіз сучасних методів захисту цифрового контенту та їх застосування до тривимірних моделей, а також розробку практичного рішення у вигляді плагіна для програми Blender.

У процесі дослідження виявлено, що захист 3D моделей стає все більш актуальною задачею у зв'язку з розвитком комп'ютерних технологій та зростанням числа цифрових творів. Застосування сучасних методів стеганографії та цифрових водяних знаків, зокрема алгоритм Коха та Жао, демонструють високу ефективність у захисті авторських прав, забезпечуючи стійкість до атак та збереження якості зображення.

Аналіз економічних, юридичних та етичних аспектів підкреслив важливість захисту інтелектуальної власності як для індивідуальних творців, так і для компаній, що інвестують у розробку цифрових продуктів. Практична реалізація розробленого плагіна для Blender підтвердила можливість впровадження передових технологій у повсякденну практику, забезпечуючи автоматизовану охорону інтелектуальної власності.

Плагін реалізовано для платформи Blender, оскільки вона відзначається не лише потужним функціоналом у галузі тривимірного моделювання, але й активною спільнотою розробників та підтримкою відкритого програмного коду. Вибір Blender підкріплюється порівнянням з іншими платформами, що дозволяє зрозуміти переваги використання даного інструменту для реалізації задачі захисту інтелектуальної власності у контексті 3D моделювання. У перспективі планується модифікувати створений плагін, щоб зробити його більш зручним і функціональним. Також буде додано ще декілька методів захисту проектів, що унеможливить несанкціонований доступ до файлів.

Список літератури

1. Watermarking 3D Models: A Comprehensive Guide URL: https://www.researchgate.net/publication/224725105_Watermarking_3D_models.
2. Актуальність методів захисту 3D проектів URL: https://inmad.vntu.edu.ua/portal /static/D8C3236E-DFEF-4A14-87A6-8A71AB8DE59D.pdf
3. Courtney K. K. Digital Rights Management: The Librarian's Guide. Rowman & Littlefield Publishers. 2016.
4. Кулик М. Дослідження сучасних алгоритмів побудови цифрових водяних знаків для відео-контенту. URL: https://ela.kpi.ua/server/api/core/bitstreams/9d614fb3-27e3-4059-8392-3f0d76f32b1b/content

5. Реута Г. Забезпечення цілісності даних з використанням цифрових підписів і сертифікатів. URL: https://ela.kpi.ua/server/api/core/bitstreams/04f65f51-8ee4-4e42-a012-02d09585fc45/content
6. Створення доповнення (аддону) для Blender. URL: https://blender3d.com.ua/sozdaniye-dopolneniya-addona-dlya-blender/
7. Create your first Blender add-on. URL: https://community.osarch.org/discussion/759/blender-create-your-first-blender-add-on
8. Rubel A.S, Fedorov A. Detection of Hidden Data Embedded by the Koch and Zhao Method. *International conference on advanced information and communication technologies*. *Lviv, Ukraine* . 2015. P. 147-148.

DEVELOPMENT OF A PLUGIN FOR BLENDER TO PROTECT INTELLECTUAL PROPERTY IN 3D MODELING

A. Lozovskyi, N. Kushnirenko, V. Nazarov, V. Podufalov

National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine;
email: infsec2011@gmail.com

This work is dedicated to the analysis of issues related to the protection of intellectual property rights in three-dimensional models. In the modern world, 3D modeling has gained wide popularity and application in various fields, including the film industry, video games, medicine, architecture, and manufacturing. The rapid development of 3D printing technologies and digital platforms creates new opportunities but also new challenges for rights holders. One of the key issues is the proliferation of illegal copying and use of 3D models, which can lead to significant financial losses for authors and companies investing in the development of such models. Traditional legal mechanisms of protection such as copyright, patents, and trademarks do not always effectively operate in the digital environment where rights violations can occur instantaneously and on a global scale. The article discusses various approaches to protecting intellectual property in 3D models. Specifically, it analyzes the possibilities of using digital watermarks, cryptographic methods, and other technological means to safeguard against illegal copying and distribution. The outcome of the work is a developed plugin for the Blender software, which provides automatic protection of copyrights on final images by applying digital watermarks. Using the developed plugin, an author can invisibly embed their unique code into the final image. Additionally, users can verify the authorship of uploaded images. This solution can find broad application among creative professionals.
Keywords: protection of 3D projects, digital watermarks, plugin, intellectual property, copyright protection.

DOI 10.15276/imms.v14.no1-2.56
УДК 621.391.8

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 56-69

МОДЕЛІ ТА МЕТОДИ ОБРОБКИ СИГНАЛІВ НА ФОНІ КОРЕЛЬОВАНИХ АСИМЕТРИЧНИХ ПРОЦЕСІВ

В.В. Палагін[1], Д.О.Смірнов[2]

[1-2]Черкаський державний технологічний університет
460, Шевченка б-р , м.Черкаси, 18006, Україна
emails: palahin@ukr.net[1], danilyyy08@gmail.com[2],

Теорія перевірки статистичних гіпотез широко застосовується в багатьох прикладних задачах, де необхідно прийняття обґрунтованих рішень на основі обмежених вибірок даних. Виявлення сигналів на фоні негаусових корельованих завад є критичним завданням у радіотехніці та телекомунікаціях, обробці зображень та біомедичних дослідженнях, де завади часто не відповідають нормальному розподілу і досліджувані вибіркові значення можуть бути статистично залежними. Статистичний підхід до розробки систем виявлення сигналів вимагає повної інформації про тип розподілу випадкових процесів, які підлягають обробці. Одним із перспективних підходів, який дозволяє описати досліджувані випадкові процеси, є використання моментного та кумулянтного опису випадкових величин. Такий підхід дозволяє суттєво спростити синтез систем виявлення зашумлених сигналів з різним типом функції розподілу. Авторами роботи запропоновано новий підхід, який грунтується на застосуванні одновимірних (1D) та двовимірних (2D) моментно-кумулянтних моделей для опису корельованих негаусових процесів, що дозволило модифікувати моментний критерій якості прийняття рішень для синтезу стохастичних поліноміальних розв'язувальних правил виявлення сигналів. В роботі продемонстровано, що нелінійна обробка вибіркових значень дозволяє врахувати тонку структуру негаусових завад у вигляді коефіцієнта асиметрії, що зменшує ймовірності помилок розв'язувальних правил у порівнянні із застосуванням традиційних гаусових моделей випадкових процеців. Метою роботи є підвищення ефективності систем виявлення сигналів при адитивній взаємодії з корельованими асиметричними негаусовими завадами на основі застосування моментно-кумулянтних моделей досліджуваних випадкових величин із формуванням модифікованого моментного критерію якості перевірки статистичних гіпотез та поліноміальних розв'язувальних правил для синтезу ефективних методів і комп'ютерних засобів обробки сигналів.

Практичне значення отриманих результатів визначається тим, що запропоновані методи та засоби моделювання дозволяють отримувати нелінійні алгоритми виявлення сигналів на фоні корельованих негаусових завад різних типів і видів з меншими ймовірностями помилок першого і другого роду порівнянно з відомими результатами. Запропоновані алгоритми відрізняються своєю нескладною практичною реалізацією і високою точністю, яка зростає при збільшенні степеня стохастичних поліномів розв'язувальних правил та врахуванні параметрів негаусових завад.

Ключові слова: перевірка статистичних гіпотез, моментно-кумулянтний опис, асиметричні корельовані нагаусові завади

Вступ. Розробка перспективних систем виявлення сигналів має велике значення для проектування та синтезу систем зв'язку, навігаційних і радіолокаційних систем, систем управління тощо [1-3]. Для розробки нових систем виявлення сигналів необхідно враховувати їх випадковий розподіл, який виникає під впливом різних типів шумів. Для розвязання ціє задачі широко використовуються класичні методи теорії перевірки статистичних гіпотез, де можна використовувати будь-яку щільність розподілу випадкових процесів [4]. Використання нормального розподілу випадкових величин набуло широкого поширення на практиці при реалізації систем виявлення сигналів. Однак у багатьох випадках відобразити реальні процеси з необхідною точністю такою моделю випадкових процесів стає неможливим. Дія на сигнали різноманітних

дестабілізуючих факторів, комплекс шумів при багатопроменевому поширенні сигналів, їх проходження через неоднорідні середовища, флуктуація параметрів зв'язку каналів породжують складну сигнально-шумову ситуацію, яка описується негаусовими випадковими процесами [5]. Використання традиційного підходу до дослідження та розробки систем обробки випадкових негаусових процесів характеризується суттєвими обмеженнями, пов'язаними зі складністю їх алгоритмічної реалізації. Складнощі з класичним підходом також пов'язані з тим, що випадкові процеси можуть бути корельованими негаусовими випадковими процесами [5]. На практиці часто виникають проблеми з обмеженим діапазоном спостережень, де не можна ігнорувати статистичні зв'язки випадкових значень випадкової величини [6].

Одним із методів вирішення поставленої задачі є метод використання функції щільності ймовірності, яка використовується для опису випадкових процесів. Запропоновано метод, заснований на пороговій системі, призначеній для виявлення детермінованого сигналу з незалежним негаусовим шумом, функції щільності ймовірності невідомі, але вони симетричні та унімодальні [7]. Цей метод підтверджено взяттям великої кількості зразків за наявності білого шуму та слабкого сигналу. Для конкретної функції щільності ймовірності, як спеціального кореляційного детектора з певними обмеженнями, представлені різні варіанти обробки сигналу [8]. На основі надпорогового стохастичного резонансу [9] нелінійний кореляційний детектор складається з узгодженого фільтра. В [10] наведено структуру субоптимального детектора з паралельним масивом двокаскадних квантувачів у негаусовому шумі. Представлено процес виявлення сигналу на основі функції щільності ймовірності в корельованому негаусовому шумі [11]. Функції щільності ймовірності обумовлені обмеженнями і труднощами в обчисленнях, хоча мають детальний опис випадкових процесів.

Показано, що властивості розв'язувальних функцій можна охарактеризувати за допомогою таких показників, як дисперсія розв'язувальних правил і середнє. Наприклад, розроблено критерій відхилення в класі лінійно-квадратичних (L-Q) систем [12-14]. Детальний опис цього критерію наведено в [15]. Але класичні критерії досить слабо пов'язані з критерієм відхилення та його модифікаціями, що не розкриває всіх властивостей правил прийняття рішень.

У роботі запропоновано інший підхід, який базується на моментно-кумулянтному описі випадкових процесів та застосуванні статистик вищих порядків (HOS - *Higher-Order Statistics*), що значно спрощує їх опис і враховує негаусову щільність розподілу.

Метою роботи є підвищення ефективності систем виявлення сигналів при адитивній взаємодії з корельованими асиметричними негаусовими завадами на основі застосування моментно-кумулянтних моделей досліджуваних випадкових величин із формуванням модифікованого моментного критерію якості перевірки статистичних гіпотез та поліноміальних розв'язувальних правил для синтезу ефективних методів і комп'ютерних засобів обробки сигналів.

1. Моментно-кумулянтні моделі корельованих асиметричних негаусових процесів. Багатовимірна функція щільності ймовірності (MD PDF - *MultiDimensional Probability Density Function*) є загальним математичним представленням статистично залежного випадкового процесу $\xi(t)$. Але PDF не завжди може бути відома і можуть виникнути деякі труднощі з оцінкою її параметрів $(\vartheta_1, \vartheta_2, \ldots, \vartheta_n)$. Для опису властивостей такого процесу можна використовувати метод, заснований на кумулянтних характеристиках [16-19]. Одновимірні (позначимо як 1D) моменти m_i випадкової величини ξ визначаються за допомогою PDF $p(\xi)$

$$E(\xi^i) = \int_{-\infty}^{\infty} \xi^i p(\xi) dx. \quad (1)$$

MD PDF може представляти статистично залежні випадкові величини [6, 20]. Дуже часто для опису статистичних характеристик зв'язку випадкових величин використовують двовимірну (2D) PDF:

$$\mathrm{E}(\xi_1{}^{\mathrm{i}}\xi_2{}^{\mathrm{j}}) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\xi_1{}^{\mathrm{i}}\xi_2{}^{\mathrm{j}}\mathrm{p}_2(\xi_1,\xi_2)\mathrm{dx}. \quad (2)$$

Можна уявити, що існують вибіркові значення стаціонарного випадкового процесу і можна розглядати окремі випадкові величини, як вибіркові значення. На практиці широко використовуваним прикладом статистично залежних значень є співвідношення для двох випадкових величин. У цьому випадку можна використовувати 2D PDF. Розглянемо випадок двох незалежних випадкових змінних ξ і η з p_ξ і p_η PDF відповідно. Тоді початкові моменти порядку i мають наступний вид:

$$m_i^{(\xi)} = E\xi^i = \int_{-\infty}^{+\infty} x^i\, p_\xi(x)dx,\ m_i^{(\eta)} = E\eta^i = \int_{-\infty}^{+\infty} y^i\, p_\eta(y)dy. \quad (3)$$

Випадкові величини ξ і η мають спільні моменти (i,j) розмірності, оскільки вони залежать один від одного. Для негаусових статистично незалежних випадкових величин (з нульовим середнім значенням та дисперсією χ_2) зв'язок між початковими моментами m_i і та кумулянтами χ_i і до четвертого порядку виглядає наступним чином:

$$m_1 = 0, m_2 = \chi_2, m_3 = \chi_3, m_4 = \chi_4 + 3\chi_2^2. \quad (4)$$

Для гаусових процесів кумулянтні коефіцієнти третього та вищих порядків $(\chi_3, \chi_4, \ \ldots)$ дорівнюють нулю. Для зв'язку між вибірками будуть використані спільні моменти $m_{i,j}$ і кумулянти $\chi_{i,j}$ до четвертого порядку включно :

$$m_{1,1} = \chi_{1,1}, m_{1,2} = \chi_{1,2}, m_{1,3} = \chi_{1,3} + 3\chi_2\chi_{1,1}, m_{2,2} = \chi_{2,2} + \chi_2^2 + 2\chi_{1,1}^2. \quad (5)$$

Зауважимо, що для задачі виявлення сигналів на фоні корельованих негаусових завад застосування моментно-кумулянтних моделей для опису досліджуваних процесів потребують додаткових досліджень та розробок. Для спрощення поставленої задачі застосуємо класифікацію досліджуваних процесів, при якій введемо певні класи кумулянтів звичайної характеристичної функції з її спільними властивостями. Така класифікація випадкових некорельованих негаусових величин отримала назву перфорованих випадкових величин [19]. В цій класифікації моментні та кумулянтні моделі представлені лише частиною кумулянтів з усіх можливих наборів, які відповідають реальному процесу. Відповідно до прийнятої класифікації розрізняють різні типи *асиметричних, ексцесних і асиметрично-ексцесних* випадкових величин [19-25].

Для вирішення поставленого завдання розроблено нові моделі негаусових корельованих випадкових процесів, що ґрунтуються на застосуванні 1D та 2D моментно-кумулянтних функцій вищих порядків. Це дозволило не лише описати негаусовий характер розподілу досліджуваних процесів, а й їх кореляційні властивості. Завдяки такому підходу стали доступними для використання такі параметри моментно-кумулянтного опису, як коефіцієнти асиметрії (γ_3) та ексцесу (γ_4), які є ненульовими у випадку негаусових моделей досліджуваних процесів.

Двовимірні статистичні зв'язки досліджуваного процесу можна представити у вигляді спільних кумулянтів $\chi_{i,j}$, які наведені в Таблиці 1. Достатньою умовою статистичної незалежності випадкових процесів є рівність нулю всіх спільних кумулянтів $\chi_{i,j}$.

Таблиця 1

Представлення двовимірних спільних кумулянтів

Порядок спільних кумулянтів	Позначення двовимірних спільних кумулянтів					
1	χ_{10}	χ_{01}				
2	χ_{20}	χ_{11}	χ_{02}			
3	χ_{30}	χ_{12}	χ_{21}	χ_{03}		
4	χ_{40}	χ_{31}	χ_{22}	χ_{13}	χ_{04}	
…	…	…	…	…	…	…

Визначення 1. Гаусовими некорельованими випадковими величинами будуть вважатися такі, які характеризуються відмінними від нуля одновимірним χ_2 і спільним χ_{11} кумулянти другого порядку, а решта кумулянтних коефіцієнтів третього та вище порядків, а також спільні кумулянти вище другого порядку дорівнюють нулю. При цьому початкові моменти до шостого порядку запишуться як:

$$\alpha_1 = \chi_1,\ \alpha_2 = \chi_2,\ \alpha_3 = 0,\ \alpha_4 = 3\chi_2^2,\ \alpha_5 = 0,\ \alpha_6 = 15\chi_2^3, \ldots,$$

а спільні моменти мають взаємозв'язок зі спільними кумулянтами:

$$m_{11}^{(v,k)} = \chi_{11} = \chi_2 \cdot r^{(v,k)},\ m_{12} = \chi_{12} = 0,\ m_{22}^{(v,k)} = \chi_2^2 + 2\chi_{11}^2 = \chi_2^2\left(1 + 2r^{(v,k)^2}\right), \ldots,$$

де $r^{(v,k)}$ - кореляційна функція заданого виду між v-м і k-м вибірковим значенням.

Зокрема, кореляційні функції можуть мати вид [6]:

$$r_\xi(\tau) = \sigma^2 e^{-A|\tau|},\ r_\xi(\tau) = \sigma^2 e^{-A|\tau|}(1 + A|\tau|),\ r_\xi(\tau) = \sigma^2 e^{-A|\tau|}(1 - A|\tau|),$$
$$r_\xi(\tau) = \sigma^2 e^{-A|\tau|}(1 + A|\tau| + A^2\tau^2/3),\ r_\xi(\tau) = \sigma^2 e^{-A|\tau|}\cos \mathrm{B}\tau, \qquad (6)$$
$$r_\xi(\tau) = \sigma^2 e^{-A|\tau|}(\cos \mathrm{B}\tau + \tfrac{A}{\mathrm{B}}\sin \mathrm{B}|\tau|),\ r_\xi(\tau) = \sigma^2 e^{-A|\tau|}(\cos \mathrm{B}\tau - \tfrac{A}{\mathrm{B}}\sin \mathrm{B}|\tau|),$$

де $\tau = |t_v - t_k|$ - кореляційний інтервал, який при врахуванні статистичних зв'язків менше інтервалу кореляції $\tau = |t_v - t_k| \le \tau_{кор}$, $v,k = \overline{1,n}$; $\tau_{кор}$ - час кореляції; $\sigma^2 = r_\xi(0)$ - дисперсія випадкового процесу; $\mathrm{A}, \mathrm{B} > 0$ – коефіцієнти, які характеризують статистичні зв'язки між вибірковими значеннями.

В роботі проводиться дослідження синтезу поліноміальних нелінійних РП виявлення сигналів, що приймається на фоні негаусових корельованих завад, які описуються коефіцієнтом асиметрії. Даний клас досліджуваного випадкового процесу представлений в таблиці 2.

Таблиця 2

Представлення двовимірних спільних кумулянтів для корельованої асиметричної негаусової величини

Порядок спільних кумулянтів	Позначення двовимірних спільних кумулянтів					
1	χ_{10}	χ_{01}				
2	χ_{20}	χ_{11}	χ_{02}			
3	χ_{30}	χ_{12}	χ_{21}	χ_{03}		

Визначення 2. Асиметричними статистично залежними випадковими величинами 1-го типу 1-го виду будемо називати такі, для яких відмінними від нуля будуть χ_2 та χ_3, а також спільні кумулянти χ_{11} та χ_{12}, а всі інші кумулянти четвертого та вище порядків, а також спільні кумулянти вище третього порядку дорівнюють нулю. У цьому випадку початкові моменти до шостого порядку мають вигляд:

$$\alpha_1 = \chi_1, \alpha_2 = \chi_2, \alpha_3 = \chi_3, \alpha_4 = 3\chi_2^2, \alpha_5 = 10\chi_2\chi_3, \alpha_6 = 10\chi_3^2 + 15\chi_2^3, \ldots,$$

а спільні моменти мають наступний взаємозв'язок зі спільними кумулянтами:

$$m_{11}^{(v,k)} = \chi_{11} = \chi_2 \cdot \rho^{(v,k)}, m_{12}^{(v,k)} = \chi_{12} = \gamma_3\chi_2^{3/2}\rho^{(v,k)^{3/2}},$$

$$m_{22}^{(v,k)} = \chi_2^2 + 2\chi_{11}^2 = \chi_2^2\left(1 + 2\rho^{(v,k)^2}\right) \ldots .$$

Прикладом *асиметричних негаусових процесів* може бути *Гамма розподіл*, який застосовується для моделювання відбитих сигналів у середовищах з багатошляховим розповсюдженням, таких як міські умови з великою кількістю будівель, де сигнали від різних шляхів можуть бути корельованими, в системах телекомунікації для опису часу життя пакету в мережах з високою затримкою, де затримки можуть бути корельованими через повторювані збої або затори в мережі.

Для *ексцесних процесів* характерний розподіл *Лапласа* для моделювання шумів у радіолокаційних системах, де шуми можуть мати піки, які значно відрізняються від середнього рівня і можуть бути корельованими через загальні джерела інтерференції. В системах телекомунікації даний вид розподілу використовується для опису втрат пакетів в мережах, де втрати можуть мати високий ексцес і бути корельованими через спільні причини втрат, такі як перевантаження мережі або апаратні збої.

До *асиметрично-ексцесних процесів* відноситься розподіл *Вейбула, Релея, Коші, розподіл Пірсона типу IV* та ін., які описують характеристики сигналів в умовах складних завад, де шуми мають як асиметрію, так і високий ексцес і можуть бути корельованими через загальні джерела завад. В системах телекомунікації моделюють інтервали затримки передачі пакетів у мережах з великим навантаженням, де затримки можуть мати одночасно асиметрію, високий ексцес і бути корельованими через спільні мережеві умови. Також такі процеси застосовуються для моделювання амплітуд сигналів у безпосередньому радіолокаційному зв'язку, де сигнали можуть бути корельованими через загальні траєкторії розповсюдження та ін.

Виявлення сигналів на фоні негаусових корельованих завад є важливою задачею в різних технічних галузях. Зокрема, виявлення об'єктів з низькою ефективною площею розсіювання (наприклад, дронів або стелс-літаків) у складних умовах завад від землі або води, де завади мають негаусовий характер і корельовані через повторювані відбиття [26, 27]. До таких задач відноситься виявлення та декодування сигналів мобільних пристроїв у міських умовах, де завади від численних джерел, таких як будівлі та інші інфраструктурні об'єкти, мають негаусовий характер та є корельованими. Виявлення природних сейсмічних подій (землетрусів) в умовах міських або промислових зон, де завади від людської діяльності (транспорт, промислові машини) мають негаусовий характер і корельовані через повторюваність діяльності [28]. Виявлення аномальних серцевих ритмів на фоні негаусових корельованих завад, які можуть виникати через артефакти руху або м'язову активність [29]

В даній роботі пропонується розробка нових моментно-кумулянтних моделей статистично залежних асиметричних негаусових випадкових величин. На основі цих моделей створені нові методи виявлення сигналів з використанням модифікованого моментного критерію якості перевірки статистичних гіпотез [22]. Такі методи відрізняються від існуючих, використовують багатовимірні моментно-кумулянтні функції вищих порядків (HOS) для врахування тонкої структури негаусових корельованих випадкових процесів. Такий підхід буде використаний для синтезу поліноміальних стохастичних розв'язувальних правил (РП) для виявлення сигналів на фоні корельовани асиметричних негаусових завад.

2. Адаптованний моментний критерій якості прийняття рішень для побудови поліноміальних розв'язувальних привил. Нехай випадкові сигнали $\xi(t)$ спостерігаються на інтервалі часу $(0, T)$. Необхідно розробити алгоритми обробки стохастичних процесів ξ(t) для прийняття рішення: стохастичні процеси містять корисний сигнал $s(t)$ (реалізується гіпотеза H_1) або корисний сигнал відсутній і випадкові процеси $\xi(t)$ містять тільки заваду $\eta(t)$ (реалізується гіпотеза H_0), де $\xi(t) = s(t) + \eta(t)$, $\eta(t) -$ стаціонарний корельований асиметричний негаусовий випадковий процес, який описується набором 1D та 2D кумулянтів і моментів.

Будемо вважати, що множина моментів при реалізації гіпотези H_1 матиме вигляд - $(m_i^{(v)}, m_{i,j}^{(\tau)})$, а для гіпотези H_0 -$(u_i^{(v)}, u_{i,j}^{(\tau)})$, де $\{u_i^{(v)}, m_i^{(v)}\}$ - 1D моменти в момент часу t_v порядку i та $\{\{u_{i,j}^{(\tau)}, m_{i,j}^{(\tau)}\}$ - 2D спільні моменти розмірності (i,j) при реалізації гіпотези H_0 і H_1 відповідно.

На практиці іноді зручніше опрацьовувати не неперевний сигнал, а дискретний. В цьому випадку дискретна вибірка сигналу $\xi(t)$ буде мати вид $\boldsymbol{X} = \{x_1, x_2, \dots, x_n\}$ в моменти часу t_v для гіпотези H_0 and H_1 наступним чином:

$$H_i: \xi_v = s_v(\alpha_k) + \eta_v\left(\gamma_k, \chi_{i,j}^{(\tau)}\right),$$

$$H_0: \xi_v = \eta_v\left(\gamma_k, \chi_{i,j}^{(\tau)}\right), v = \overline{1,n}. \quad (7)$$

де $s_v(\alpha_k)$ – корисний сигнал, який описується параметрами α_k, $\eta_v\left(\gamma_k, \chi_{i,j}^{(\tau)}\right)$ – негаусова випадкова величина з параметрами у формі набору кумулянтів $\chi_{i,j}^{(\tau)}$, $k = \overline{1,\mu}$.

Відповідно до класичного підходу, оптимальний Байєсівський алгоритм виявлення сигналів мінімізує середній ризик [1-3]. Достатня статистика, яка необхідна для перевірки гіпотези, визначається як відношення правдоподібності і має вид

$$\Lambda(\boldsymbol{X}) = P(\boldsymbol{X}|H_1)/P(\boldsymbol{X}|H_0). \quad (8)$$

Як правило, таке відношення правдоподібності в більшості випадків інтерпритується для нормальних законів розподілу щільності ймовірності. Разом з тим, отримання розв'язків у форматі рівняння (8) для негаусових корельваних PDF створює алгоритмічні труднощі, пов'язані з невизначеністю параметрів PDF, технічною складнісю їх реалізації. Отже, потрібні альтернативні підходи, щоб обійти ці проблеми. Один із таких альтернативних підходів може полягати у вираженні відношення правдоподібності, як степеневої поліноміальної функції [6, 19-25].

Припустимо, що відношення правдоподібності (8) є неперервною функцією та може бути представлено як стохастичний степеневий поліном степіня s для випадкових вибірок x_v:

$$\Lambda(x_1, x_2, \dots, x_n) = k_0 + \sum_{i=1}^{\infty}\sum_{v=1}^{n} k_{iv}\phi_i(x_v), \quad (9)$$

де функції $\phi_i(x_v)$ представляють перетворення вибіркових значень x_v, які можуть включати степеневі або тригонометричні функції. Коефіцієнти k_{iv} та k_0 є невідомими параметрами, обраними на основі відповідного критерію якості. Крім того, якщо функції $\phi_i(x_v)$ є лінійно незалежними і утворюють базис, тоді для широкого класу функцій $\Lambda(\boldsymbol{X}) = f(x_1, x_2, \dots, x_n)$ розкладання у вигляді ряду (9) є можливим.

На практиці замість нескінченних рядів (9) використовуються поліноми зі скінченним числом доданків *s*. Тоді вираз (9) при степеневому перетворенні вибіркових значень x_v прийме вид степеневого стохастичного полінома степеня *s*:

$$\Lambda(\boldsymbol{X}) = \sum_{v=1}^{n}\sum_{i=1}^{s} k_{iv}\, x_v^i + k_0, \quad (10)$$

де оптимальні коефіцієнти k_{iv} та k_0 такого РП мають визначатися згідно заданого критерію якості. В якості критерія перевірки статистичних гіпотез обраний модифікований моментний критерій якості [22], який враховує статистичні зв'язки вибіркових значень:

$$Ku(E,G) = \frac{G_0[\gamma] + G_1[\gamma]}{(E_1[\gamma] - E_0[\gamma])^2}. \quad (11)$$

Критерій $Ku(E,G)$ (11) визначає якісні характеристики прийняття рішень РП (10). Цей критерій будемо називати «Модифікований моментний критерій якості верхніх границь ймовірностей помилок» або коротко критерієм «Ku».

Оскількі значення стохастичного поліноміального РП (10) є випадковими, тоді характеристиками такого РП будуть математичне сподівання $E_{0(sn)}$, $E_{1(sn)}$ та дисперсія $\mathrm{G}_{0(\mathrm{sn})}$, $\mathrm{G}_{1(\mathrm{sn})}$ при гіпотезі H_0 та H_1 відповідно:

$$E_{0(sn)} = \sum_{i=1}^{s}\sum_{v=1}^{n} k_{iv} u_i^{(v)}, E_{1(sn)} = \sum_{i=1}^{s}\sum_{v=1}^{n} k_{iv} m_i^{(v)}, \quad (12)$$

$$\mathrm{G}_{0(\mathrm{sn})} = \sum_{\mathrm{i=s}}^{\mathrm{s}} \sum_{\mathrm{j=1}}^{\mathrm{s}} \sum_{\mathrm{v=1}}^{\mathrm{n}} \sum_{\mathrm{k=1}}^{\mathrm{n}} k_{iv}\, k_{jv} \mathrm{F}_{(i,j)}^{(\tau)}(\mathrm{H}_r),\ r = 0{,}1, \qquad (13)$$

де $\mathrm{F}_{(i,j)}^{(\tau)}(\mathrm{H}_0) = u_{(i,j)}^{(\tau)} - u_i^{(v)} u_j^{(k)}$, $\mathrm{F}_{(\mathrm{i,j})}^{(\tau)}(\mathrm{H}_1) = m_{(i,j)}^{(\tau)} - m_i^{(v)} m_j^{(k)}$,

і коефіцієнт k_0 буде визначатися як середнє математичних сподівань $E_{0(sn)}$, $E_{1(sn)}$ при гіпотезі H_0 та H_1 відповідно:

$$k_0 = -\frac{1}{2}\left(E_{0(sn)} + E_{1(sn)}\right) = -\frac{1}{2}\sum_{i=1}^{s}\sum_{v=1}^{n} k_{iv}(m_i^v + u_i^v), \qquad (14)$$

Відмітимо, що тонка структура досліджуваних негаусових процесів описується послідовністю моментів і кумулянтів вищих порядків (1D, HOS), а статистичні зв'язки вибіркових значень багатомірними кумулянтами (2D).

Показано, що мінімум критерію $Ku(E,G)$ (11) забезпечує мінімум суми ймовірностей помилок першого і другого роду РП (10). В цьому випадку оптимальні коефіцієнти РП (10) k_{iv} та k_0 повинні бути такими, щоб мінімізувати критерій якості $Ku(E,G)$ (11) і визначаються з наступної системи рівнянь

$$\sum_{\mathrm{j=1}}^{\mathrm{s}} k_{iv}\left(F_{i,j}^{(\tau)}(\mathrm{H}_0) + F_{i,j}^{(\tau)}(\mathrm{H}_1)\right) = m_i^{(v)} - u_i^{(v)},\ v = \overline{1,n},\ i = \overline{1,s}. \qquad (15)$$

Розв'язок даної системи рівнянь (15) не є тривіальним, де застосовуються чисельні методи при використанні допонення Шура до блочної матриці [30]. Окрім того, 2D спільні моменти $u_{(i,j)}^{(\tau)}$ та $m_{(i,j)}^{(\tau)}$ використовуються для визначення кореляційної матриці із заданою функцією кореляції $\rho^{(\tau)}$:

$$\rho^{(\tau)} = \begin{pmatrix} 1 & \rho^{(\tau_{1,2})} & \dots & \rho^{(\tau_{1,n})} \\ \rho^{(\tau_{2,1})} & 1 & \dots & \rho^{(\tau_{2,n})} \\ \dots & \dots & \dots & \dots \\ \rho^{(\tau_{n,1})} & \rho^{(\tau_{n,2})} & \dots & 1 \end{pmatrix}. \qquad (16)$$

Для проведення досліджень були використанні різні кореляційні функції (6), які мають місце в багатьох прикладних задачах [6]. Наприклад, для експоненційної кореляційної функції значення $\rho^{(\tau)}$ прийме вид:

$\rho^{(\tau_{v,k})} = e^{-A|t_v - t_k|}$, де $\tau_{v,k}$ – час кореляції, А – масштабуючий коефіцієнт.

Визначення 1. Визначимо функціонал $Ku(E,G)$ як моментний критерій якості прийняття рішень у вигляді РП (10). Припустимо, що оптимальні коефіцієнти РП k_0 (14) та k_{iv} (15), які мінімізують праву частину (11), визначають цей критерій, який називається «Модифікований моментний критерій якості верхніх границь ймовірностей помилок для перевірки статистичних гіпотез» Менше значення критерію (11) свідчить про менше значення суми ймовірностей помилок першого і другого РП (10).

Властивість 1. Якщо оптимальні коефіцієнти РП (10) визначаються розв'язуванням системи алгебраїчних рівнянь (15), тоді вони задовольняють умові

$$I_{sn} = \sum_{v=1}^{n}\sum_{i=1}^{s} k_{iv}k_{jv}\left[F_{i,j}^{(\tau)}(\mathrm{H}_0) + F_{i,j}^{(\tau)}(\mathrm{H}_1)\right] = \sum_{v=1}^{n}\sum_{i=1}^{s} k_{iv}\left(m_i^{(v)} - u_i^{(v)}\right), \qquad (17)$$

$j = \overline{1,s}$.

Визначення 2. Визначимо величину I_{sn} (17) як значення добутої інформації про розрізнення гіпотез H_0 та H_1 із вибірки розміром *n* при використанні стохастичного поліноміального РП (10) степені s.

Властивість 2. Для коефіцієнтів, визначених із системи рівнянь (15), значення критерію якості $Ku(E,G)$ (11) обернено пропорційно кількості добутої інформації про розрізнення гіпотез H_0 та H_1 із вибірки розміром *n* при використанні стохастичного поліноміального РП (10) степені *s* і виражається наступним чином:

$$I_{sn} = \frac{1}{Ku(E,G)} = \sum_{i=1}^{s}\sum_{v=1}^{n} k_{iv}\left(m_i^{(v)} - u_i^{(v)}\right). \qquad (18)$$

Значення $Ku(E,G)$ та I_{sn} може бути використано для оцінки ефективності синтезованих поліноміальних РП.

3. Синтез поліноміальних алгоритмів виявлення сигналів на фоні корельованих асиметричних негаусових завад. Нехай вхідний сигнал $\xi(t)$ складається з корисного сигналу a та завади $\eta(t)$ і спостерігається в інтервалі часу $[0, \mathrm{T}]$

$$\xi(t) = a + \eta(t), \tag{19}$$

де $\eta(t)$ - корельована стаціонарна негаусова завада з нульовим середнім і дисперсією χ_2 і описується послідовністю 1D і 2D моментів і кумулянтів.

Представимо дискретизований сигнал $\xi(t)$ як значення $\boldsymbol{X} = \{x_1,\ x_2, \dots, x_n\}$ в моменти часу t_v для гіпотези H_i $(i = 0{,}1)$ в наступній формі:

$$H_1\colon x_v = a + \eta_v\left(\gamma_k, \chi_{i,j}^{(\tau)}\right),$$

$$H_0\colon x_v = \eta_v\left(\gamma_k, \chi_{i,j}^{(\tau)}\right),\ v = \overline{1,n}. \tag{20}$$

Розглянемо поліноміальне РП для степені s=1. Показано, що алгоритм виявлення сигналу в корельованому негаусовому шумі з використанням РП (10) за першим степенем полінома s=1 має вигляд

$$\sum_{v=1}^{n} A_v \left(x_v - \frac{a}{2}\right) \underset{H_0}{\overset{H_1}{\gtrless}} 0, \tag{21}$$

де A_v - визначник, який отримується з Δ_1, коли v -й стовпець замінюється одиницями, а Δ_1 визначається з виразу

$$\Delta_1 = det\left\|F_{(1,1)}^{(\tau)}\right\| = det\left\|\rho^{(\tau_{v,k})}\right\|,\ v,k = \overline{1,n}, \tag{22}$$

де $F_{(i,j)}^{(\tau)} = F_{(i,j)}^{(\tau)}(H_0) + F_{(i,j)}^{(\tau)}(H_1)$.

Як вже відзначалося, ефективність синтезованих РП може оцінюватися за двома характристиками - $Ku(E,G)$ (11) та I_{sn} (18). Показано, що для отриманого РП (21) кількість добутої інформації про розрізнення гіпотез H_0, H_1 має вид

$$I_1 = \frac{q}{\Delta_1}\sum_{v=1}^{n} A_v \tag{23}$$

і є оберненою величиною до критерію якості прийняття рішеня $Ku(E,G)$ (11), де $q = a^2/\chi_2$ – відношення сигнал/шум (SNR - *signal-to-noise ratio*).

Легко показати, що для стаціонарного статистично незалежного процесу, коли не враховуються 2D моменти та кумулянти для опису випадкових величин, значення критерію $Ku(E,G)$ перетворюється в наступну форму

$$Ku_1(E,G) = 2/nq, \tag{24}$$

а РП (21) трансформується в добре відоме лінійне класичне правило виду

$$\frac{1}{n}\sum_{v=1}^{n} x_v - \frac{a}{2} \underset{H_0}{\overset{H_1}{\gtrless}} 0. \tag{25}$$

Відмітимо, що отриманий результат у вигляді лінійного РП (21) не враховує негаусовий розподіл випадкового процесу, оскільки для його опису використовувалися лише перші два початкові моменти.

Збільшимо степінь полінома РП (10) до s=2. Тоді РП буде нелінійним і в загальному випадку матиме вигляд

$$\sum_{v=1}^{n} k_{1v}x_v + \sum_{v=1}^{n} k_{2v}x_v^2 + k_0 \underset{H_0}{\overset{H_1}{\gtrless}} 0, \quad (26)$$

де оптимальні коефіцієнти k_{iv} визначаються із системи рівнянь (15) і мають наступний вигляд

$$k_{1v} = \frac{B_v}{\Delta_2},\ v = \overline{1,n},\ k_{2v} = \frac{C_v}{\Delta_2},\ v = \overline{n+1,\ 2n}, \quad (27)$$

де B_v – визначник, який отриманий з визначника Δ_2, коли v -й стовбець ($v = \overline{1,n}$) замінений на інший зі значеннями $(q^{0.5}, q^{0.5}, \dots, q^{0.5} \quad q, q, \dots, q)$, C_v – визначник, який визначається подібним чином для $v = \overline{n+1,\ 2n}$, де Δ_2 має вид

$$\Delta_2 = det \begin{vmatrix} \left\| F_{1,1}^{(\tau_{v,k})} \right\| & \left\| F_{1,2}^{(\tau_{v,k})} \right\| \\ \left\| F_{2,1}^{(\tau_{v,k})} \right\| & \left\| F_{2,2}^{(\tau_{v,k})} \right\| \end{vmatrix},\ v,k = \overline{1,n}. \quad (28)$$

Показано, що в цьому випадку загальний вид порогового коефіцієнта k_0 РП (26) для отриманих коефіцієнтів k_{1v} and k_{2v} розраховується як

$$k_0 = -\frac{1}{2\Delta_2}\sum_{v=1}^{n}\left(q^{0.5}B_v + C_v(q+1)\right). \quad (29)$$

Показано, що нелінійне РП (26) враховує характеристики корельованого негаусового процесу у формі коефіцієнтів асиметрії γ_3 та спільних кумулянтів $\chi_{i,j}^{(\tau)}$, $i,j = \overline{1,2}$.

Значення добутої інформації з вибіркових значень про розрізнення гіпотез H_0, H_1 при використанні РП (26) визначається як

$$I_2 = \frac{1}{\Delta_2}\sum_{v=1}^{n}(q^{0.5}B_v + qC_v). \quad (30)$$

Відмітимо, що можливий синтез нелінійних поліноміальних РП більших степінів, де будуть враховані моменти та кумулянти вищих порядків. В цьому випадку потрібно знаходити компроміс між збільшенням ефективності синтезованих РП, ускладненням обчислювальних процесів та звуженням області допустимих значень для кумулянтних коефіцієнтів вищих порядків [19].

4. Результати та обговорення. Отримані математичні моделі корельованих асиметричних негаусових випадкових процесів і застосування стохастичних поліноміальних РП, оптипальних по модифікованому моментному критерію якості верхніх границь ймовірностей помилок для перевірки статистичних гіпотез дозволяють підвищити ефективність обробки сигналів у порівнянні з добре відомими гаусовими моделями.

Отримані результати залежать як від виду кореляційних функцій, які досліджувалися, так і від характеристик асиметричного негаусового процесу. На рис.1 предслені найбільш поширені кореляційні функції (6) [6], які досліджувалися в роботі. В якості параметрів кореляційних функцій використовивулися різні масштабуючі коефіцієнти «А» і «В». Малі значення параметрів «А» і «В» (порядку 0.1) характеризують наявність сильних статистичних зв'язків між вибірковими значеннями, і для великих значень (більше 1) – слабкі. При зростанні цих апарметрів процес вироджується в статистично незалежний.

На рис.2 представлені залежності значення критерію Ku (11) для РП при степені s=1 (21) від відношення сигнал/шум (q - SNR) при різних кореляційних функціях для випадків, коли розглядаються корельовані і не корельоваі випадкові процеси. В даному випадку значення критерію Ku є зворотною величиною кількості добутої інформації про розрізнення гіпотез I_1 (23). При першій степені полінома для опису статистичних

властивостей випадкового процесу враховуються тільки перших два початкових моменти. Відповідно, такі РП характеризують тільки гаусові процеси при різних значеннях кореляційних функцій (6) з відповідними масштабуючими коефіцієнтами «А» і «В».

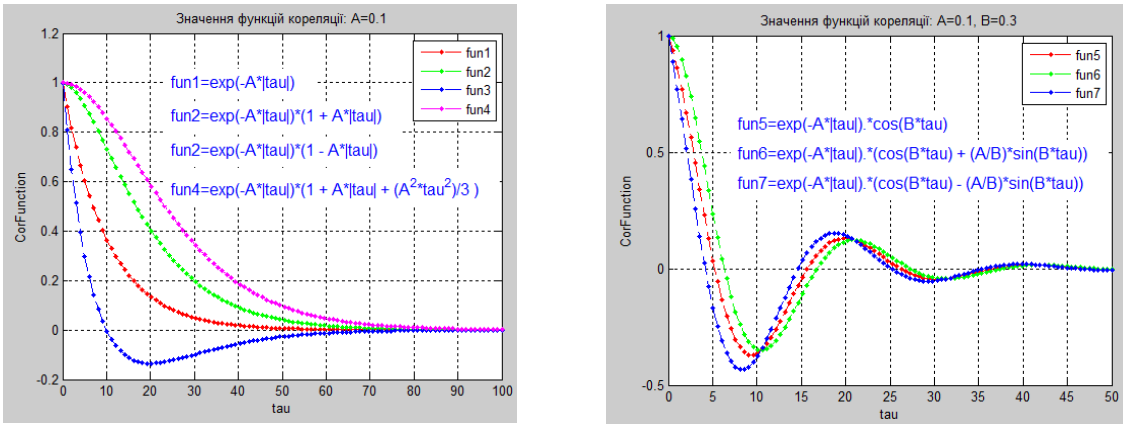
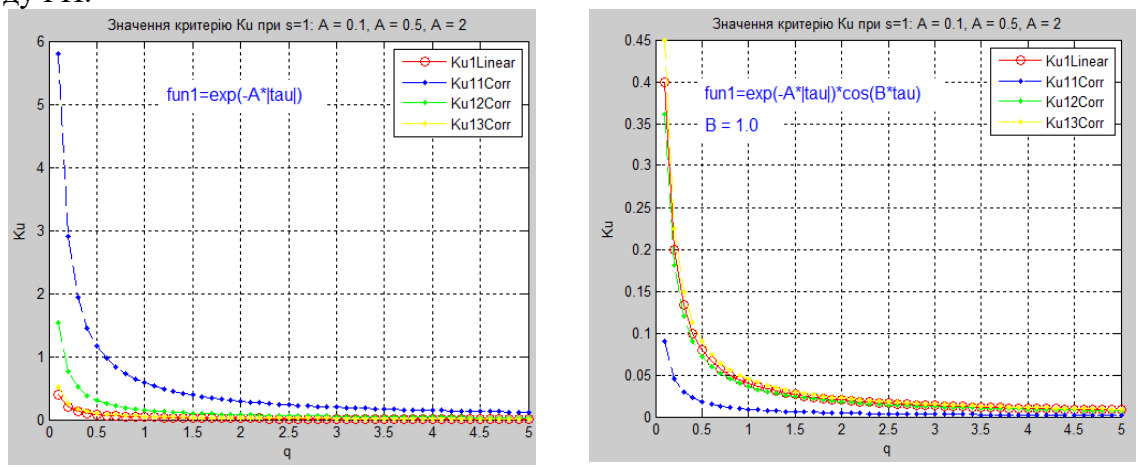


Рис.1. Представлення значення кореляційних функцій з масштабучими параметрами «А» і «В» від інтервалу кореляції tau.

На рис.2. Ku1Linear характеризує значення критерію Ku_1 (24) для статистично незалежних вибіркових значень (A>1), а Ku11Cor, Ku12Cor, Ku13Cor значення критерію при різних параметрах A=0.1, 0.5, 2.0 відповідно. Для статистично незалежних вибіркових значень величина критерію вироджується у вираз Ku_1 (24) і обернено пропорційно залежить від кількості вибіркових значень n і параметра q, а лінійне РП (21) вироджується у добре відомий вираз (25). З графіків видно, що при зростанні відношення сигнал/шум q значення критерію Ku_1 зменшується, що свідчить про зменшення ймовірностей помилок першого і другого роду лінійного РП (21). Необхідно відмітити, що наявність кореляційних зв'язків погіршує ефективність РП (рис.2 - а), але можуть бути такі кореляційні функції (рис.2 - б), коли нявність статистичних зв'язків зменшує значення критерію Ku_1, а відповідно, зменшує ймовірності помилок першого і другого роду РП.

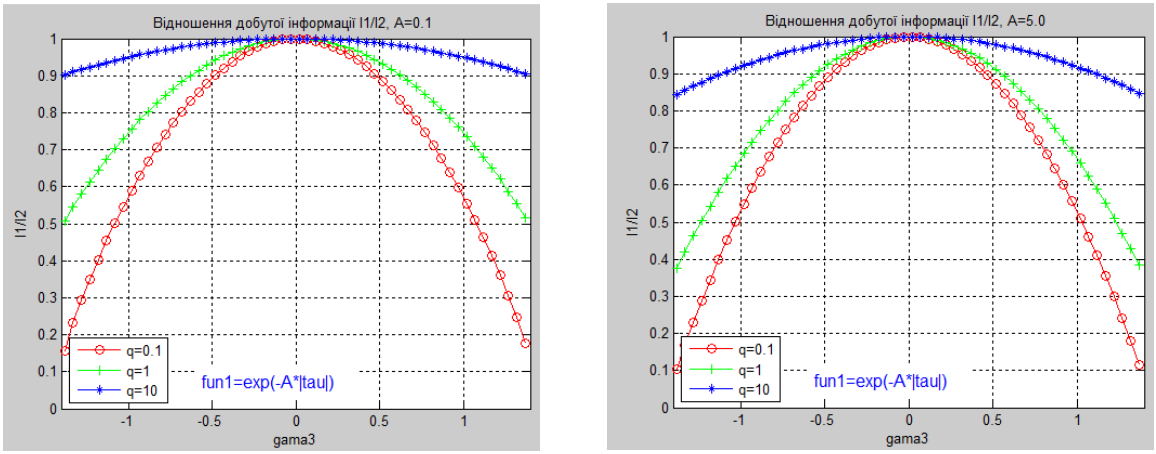


а) б)

Рис.2. Залежність значення критерію Ku для РП при степені s=1 від відношення сигнал/шум q при n=100.

На рис.3 представлені залежності відношення кількості добутої інформації I_1 (23) про розрізнення гіпотез для лінійного РП при степені полінома s=1 (21) до кількості добутої інформації I_2 (30) про розрізнення гіпотез для нелінійного РП при степені полінома s=2 (26) від коефіцієнта асиметрії негаусової завади при різних значеннях відношення сигнал/шум q і параметрах кореляції «А». Як показано на графіках,

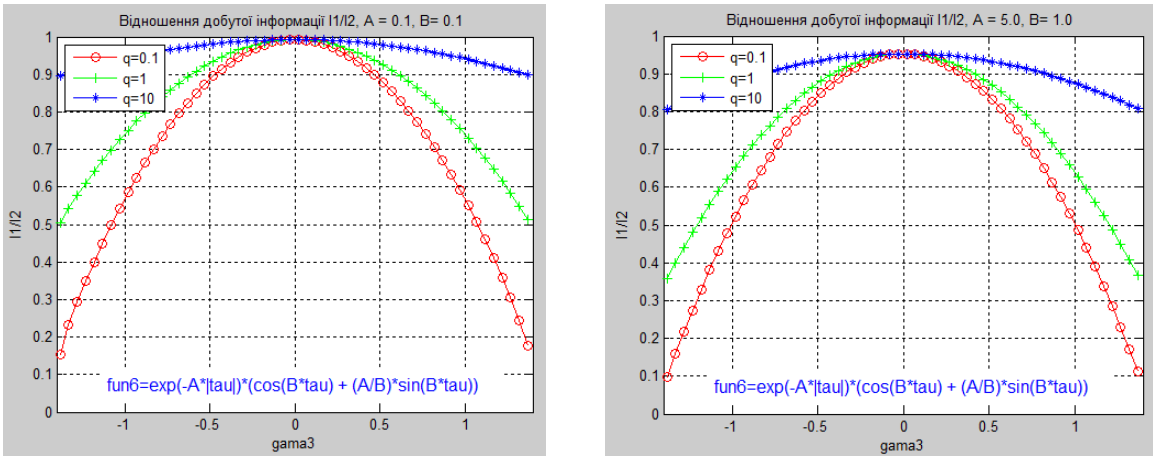
врахування параметра асимтерії негаусової завади gama3 дозволяє збільшити значення кількості добутої інформації про розрізнення гіпотез для нелінійного РП (26) у порівнянні з лінійним (21), що підвищує ефективність виявлення сигналів. Так, при значенні gama3=1.1 (рис.3-а) значення I_2 буде удвічі перевищувати I_1, а відповідно, ймовірності помилок таких РП теж будуть удвічі менше у порівняні з лінійним РП, яке є оптимальним для гаусових моделей завад.



а) б)

Рис.3. Залежність відношення I_1/I_2 від коефіцієнта асиметрії негаусової завади gama3 при різних значеннях відношення сигнал/шум q і параметрах кореляції «А» для кореляційної функції $r_\xi(\tau) = \sigma^2 e^{-A|\tau|}$.

При зміні функції кореляції (рис.4) загальні тенденції підвищення ефективності нелінійної обробки у порівнянні з лінійною зберігаються як для сильних статистичних звязків (а), так і для послаблених (б).



а) б)

Рис.4. Залежність відношення I_1/I_2 від коефіцієнта асиметрії негаусової завади gama3 при різних значеннях відношення сигнал/шум q і параметрах кореляції «А» і «В» для кореляційної функції $r_\xi(\tau) = \sigma^2 e^{-A|\tau|}(cos\,\mathrm{B}\,\tau + \frac{A}{\mathrm{B}} sin\,\mathrm{B}\,|\tau|)$.

5. Висновки. Обробка зашумлених сигналів є значною статистичною проблемою для багатьох практичних застосувань. Основою для вирішення цих проблем є використання відношення прадоподібності. Однак, застосування цього підходу до корельованих негаусових моделей випадкових процесів представляє практичні труднощі, пов'язані з визначенням типу щільності розподілу, його параметрів, а також синтезом і аналізом алгоритмів. У статті запропоновано альтернативний підхід до опису випадкових

процесів, який заснований на використанні моментів і кумулянтів, нескінченна послідовність яких дозволяє точно наблизити запропонований опис випадкових величин до повного імовірнісного опису.

В роботі розроблені нові моделі корельованих асиметричних негаусових процесів, які використано для побудови поліноміальних стохастичних РП, оптимальні коефіцієнти яких визначаються з нового «Модифікованого моментного критерію якості верхніх границь ймовірностей помилок для перевірки статистичних гіпотез».

На основі запропонованого підходу були синтезовані лінійні та нелінійні РП, досліджені їх властивості та отримані характеристики, які показують їх ефективність при впливі корельованих асиметричних негаусових завад. Показано, що лінійні РП не враховують негаусовий розподіл випадкових величин. Це пояснюється тим, що для їх опису використовуються лише перші два моменти, що представляють середнє значення та дисперсію випадкових процесів. Але отримані лінійні РП збігаються з тими, що отримані з відношення правдоподібності для гаусових моделей випадкових величин.

Нелінійна обробка вибіркових значень та врахування статистик вищих порядків негаусових процесів у вигляді коефіцієнта асимтерії призводить до покращення ефективності системи виявлення сигналів, що проявляється у зменшенні значення критерію якості РП, і відповідно, зменшенні ймовірностей помилок першого та другого роду таких РП. Показано, що вплив кореляційних зв'язків зменшує ефективність обробки, яка зменшується як для лінійних, так і нелінійних РП, але врахування структури негаусового прооцесу у вигляді коефіцієнта асиметрії в цілому покращує роботу нелінійної обробки РП.

Список літератури

1. Van Trees H., Bell K., Tiany Z. Detection Estimation and Modulation Theory. New Jersey: Wiley, 2013.
2. Kay S.M. Fundamentals of Statistical Signal Processing. NJ: Prentice Hall PTR, 2008.
3. Lin C., Chang Q., Li X. A Deep Learning Approach for MIMO-NOMA Downlink Signal Detection. *Sensors.* 2019. V.19. P.2526. URL: https://doi.org/10.3390/s19112526.
4. Michael H. Herzog, Francis G., Clarke A. Experimental Design and the Basics of Statistics: Signal Detection Theory (SDT). New York: Springer Verlag, 2019. URL: https://doi.org/10.1007/978-3-030-03499-3.
5. Kassam S. Signal Detection in Non-Gaussian Noise. New York: Springer Verlag, 2011.
6. Палагін В. В., Івченко О. В. , Вєдєрніков Д. А. Статистичне оцінювання параметрів негаусових корельованих випадкових процесів :монографія. Черкаси: ФОП Гордієнко Є.І., 2018. 199 с.
7. Guo G., Mandal M., Jing Y. A robust detector of known signal in non-Gaussian noise using threshold systems. *Signal Processing*. 2012. V. 92. No.11. P. 2676-2688. URL: https://doi.org/10.1016/j.sigpro.2012.04.014.
8. Duana F., Chapeau-Blondeau F., Abbott D. Non-Gaussian noise benefits for coherent detection of narrow band weak signal. *Physics Letters. A*. 2014. V. 378.. P.1820–1824. URL: https://doi.org/10.1016/j.physleta.2014.04.061.
9. Hari V.N., Anand G.V., Premkumar A.B., Madhukumar A.S.: Design and performance analysis of a signal detector based on suprathreshold stochastic resonance. *Signal Processing*. 2012. V.92. No 6. P.1745–1757. URL: https://doi.org/10.1016/j.sigpro.2012.01.013.
10. Rousseau D., Anand G.V., Chapeau-Blondeau F.: Noise enhanced nonlinear detector to im-prove signal detection in non-Gaussian noise. *Signal Processing*. 2006. V. 86. No. P. 3456–3465. URL: https://doi.org/10.1016/j.sigpro.2006.03.008.
11. Izzo L., Tanda M. Asymptotically optimum diversity detection in correlated non-Gaussian noise. *IEEE Transactions on Communication*. 1996. V. 44. No 5. P. 542 - 545. URL: https://doi.org/10.1109/26.494296.

12. Picinbono B.: On deflection as a performance criterion in detection. *IEEE Trans. Aerosp. Electron. Syst*. 1995. V. 31. No. 3. P.1072–1081. URL: https://doi.org/10.1109/7.395235.
13. Vachkov G. Online detection of deviation in performance of multichannel dynamical processes. *Mathematical Modelling of Signal Detection in Non-gaussian Correlated Noise*. 2016. No.5. P.1681–1686. URL: https://doi:10.1109/ICMA.2013.6618168.
14. Solc T, Mohorcic M, Fortuna C. A methodology for experimental evaluation of signal detection methods in spectrum sensing. *PLoS ONE* . 2018. V.13(6). P.1-31. URL: https://doi.org/10.1371/journal. pone.0199550.
15. Biglieri E., Lops M. Linear–Quadratic Detectors for Spectrum Sensing. *Journal of Communications and Networks*. 2014. V. 16. No.5. P. 485-492. URL: https://doi.org/10.1109/JCN.2014.000087.
16. Peppas K., Mathiopoulos P., Yang J., Zhang C., Sasase I. High-order statistics for the channel capacity of egc receivers over generalized fading channels. *IEEE Communications Letters*. 2018. V. 22. No. 8. 1740-1743. URL: https://doi.org/10.1109/LCOMM.2018.2846229
17. Watts J. P., Smith P. Stochastic Processes. An Introduction. Third Edition. 2018. Chapman and Hall/CRC.
18. Jammalamadaka S., Taufer E., Terdik, G.. Cumulants of Multivariate Symmetric and Skew Symmetric Distributions. *Symmetry*. 2021. V.13, P.1383. URL: https://doi.org/10.3390/sym13081383.
19. Kunchenko Y. Polynomial Parameter Estimations of Close to Gaussian Random Variables. Aachen: Shaker Verlag, 2002.
20. Vokorokos L., Marchevsky S., Ivchenko A., Palahina E., Palahin V.: Parameters Estimation of Correlated non-Gaussian processes by the Method of Polynomial Maximization. *IET Journal* 2017. V. 11. No.3, P.313–319. URL: https://doi.org/10.1049/iet-spr.2016.0142.
21. Palahin V., Juhar, J., Leleko S., Polozhaenko S., Palahina E. Computer Simulation of Signal Detection in non-gaussian Noise with the Neyman-Pearson Moment Quality Criterion. *9th International IEEE Conference Dependable Systems, Services and Technologies DESSERT*. 2018, P.639-644. URL: 2018. https://doi.org/10.1109/DESSERT.2018.8409203.
22. Palahina E., Gamcova M., Gladisova I., Gamec J., Palahin V.: Signals Detection in Correlated non-Gaussian Noise Using Higher-Order Statistics. *Circuits, Systems, and Signal Processing,* 37(4), 1704-1723 (2018). https://doi.org/10.1007/s00034-017-0623-5.
23. Palahin V., Juhar, Z., O., Viediernikov D., Palahina E.: Computer Modeling of Noise Signals Proccesing System in non-Gaussian Noise. *IEEE 38th International Conference on Electronics and Nanotechnology (ELNANO, Kiev)*. 2018. P.658-662.
24. Д.О. Смірнов, Д.А. Ведерников, О.А. Палагіна, В.В. Палагін. Методи статистичного оцінювання параметрів сигналу на фоні негаусових корельованих завад. *Математичне та комп'ютерне моделювання. Серія: Технічні науки*. 2021. Т 22. С.106-118.
25. Палагін В.В., Зорін О.С. Моделі та методи розрізнення RZ-сигналів в інформаційно-вимірювальних системах на фоні асиметричних негаусових завад. *Вісник Вінницького політехнічного інституту.* 2023. №4. С.78–86. URL: https://doi.org/10.31649/1997-9266-2023-169-4-78-86
26. Guo G., Mandal M., Jing Y. A robust detector of known signal in non-Gaussian noise using threshold systems. *Signal Processing*. 2012. V. 92, No.11. P.2676-2688.
27. Chen Ch., Xu W., Pan Y., Zhu H., Wang J. A Nonparametric Approach to Signal Detection in Non-Gaussian Noise, *IEEE Signal Processing Letters*, vol.29, pp.503-507. (2022)
28. Zhong T., Li Y., Wu N., Nie P., Yang B. Statistical analysis of background noise in seismic prospecting. *Geophysical Prospecting.* 2015. V. 63, No 5. P.1161-1174.

29. Hai B.H. Enhanced ECG Record Quality: Integrated Artifact Suppression Using Soft Threshold on Wavelet Coefficients and Adaptive Filter Model. *Mathematical Modelling of Engineering Problems*. 2023. V. 10, No. 3. P.871-878.
30. Horn R.A., Johnson C.R. Matrix Analysis, second edition. Cambridge University Press, 2013.

MODELS AND METHODS OF SIGNAL PROCESSING IN CORRELATED ASYMMETRIC PROCESSES

V.V.Palahin[1], D.O.Smirnov [2]

[1-2]Cherkasy State Technological University
460, Shevchenko blvd., Cherkasy, 18005, Ukraine,
emails: palahin@ukr.net[1], danilyyy08@gmail.com[2]

The theory of statistical hypothesis testing is widely used in many applied problems where it is necessary to make informed decisions based on limited data samples. Signal detection in correlated non-Gaussian noise is a critical task in radio engineering and telecommunications, image processing, and biomedical research, where the noise often does not follow a normal distribution and the sample values under study may be statistically dependent. A statistical approach to the development of signal detection systems requires complete information about the type of distribution of random processes to be processed. One of the promising approaches that allows describing the studied random processes is the use of moment and cumulant description of random variables. This approach makes it possible to significantly simplify the synthesis of noisy signal detection systems with different types of distribution functions. The authors of the paper proposed a new approach based on the application of one-dimensional (1D) and two-dimensional (2D) moment-cumulant models for describing correlated non-Gaussian processes, which made it possible to modify the moment criterion of decision-making quality for the synthesis of stochastic polynomial solving rules for signal detection. The work demonstrated that nonlinear processing of sample values allows taking into account the subtle structure of non-Gaussian disturbances in the form of an asymmetry coefficient, which reduces the probability of errors in the solving rules compared to the use of traditional Gaussian models of random processes. The aim of the work is to improve the efficiency of signal detection systems in the case of additive interaction with correlated asymmetric non-Gaussian noise based on the application of moment-cumulant models of the studied random variables with the formation of a modified moment quality criterion for testing statistical hypotheses and polynomial solving rules for the synthesis of effective methods and computer tools for signal processing. The practical value of the obtained results is determined by the fact that the proposed methods and modeling tools allow obtaining nonlinear algorithms for signal detection in correlated non-Gaussian noise of various types with lower probabilities of errors of the first and second kind compared to known results. The proposed algorithms are distinguished by their simple practical implementation and high accuracy, which increases when the degree of stochastic polynomials of the solving rules increases and the parameters of non-Gaussian noise are taken into account.

Keywords: statistical hypothesis testing, moment-cumulant description, asymmetric correlated non-Gaussian noise

DOI 10.15276/imms.v14.no1-2.70
УДК 004.85

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp.70-84

ЗАСТОСУВАННЯ МЕТОДУ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ ШКІДЛИВОГО МЕРЕЖЕВОГО ТРАФІКУ НА КАНАЛЬНОМУ РІВНІ (ARP-атаки)

В.В. Палагін[1], О.А. Палагіна[2], О.В. Івченко[3], О.М. Панаско[4], Р.Л. Пташкін[5]

[1-4]Черкаський державний технологічний університет
460, Шевченка б-р, м.Черкаси, 18006, Україна
[5]Черкаський науково-дослідний експертно-криміналістичний центр МВС України,
104, Пастерівська вул., м.Черкаси, 18009, Україна
emails: palahin@ukr.net[1], palahina@ukr.net[2],
sania_ivchenko@ukr.net[3] , lena.pa@ukr.net[4], ndekc.ck@gmail.com[5]

Широке розповсюдження програмно-визначених мереж (*Software-Defined Networking* - SDN), *Internet of Things* (IoT) мереж забезпечило неперевершену гнучкість і ефективність керування мережами, але водночас поставило нові виклики у захисті мережевої інфраструктури. Однією з важливих загроз залишаються атаки підробки протоколу розпізнавання адрес (*Address Resolution Protocol* - ARP), що порушують цілісність мережі та конфіденційність даних. У цьому рукописі представлено новий підхід до виявлення ARP-спуфінгу в мережах при аналізі обмежень існуючих методологій. Проведено аналіз ARP протоколів, їх призначення та основних методів захисту від атак. Наведено типові загрози комп'ютерним мережам фізичного та канального рівнів моделі OSI та проведено аналіз особливостей виявлення таких загроз з використанням методів штучного інтелекту – ШІ (*Artificial intelligence* - AI). Запропоновано застосування методів машинного навчання (*Machine learning* - ML) для аналізу трафіку на основі отримання даних в режимі реального часу з платформи Wireshark. Новий метод базується на використанні ШІ для класифікації та виявлення зловмисного мережевого трафіку, згенерованого в результаті атак, що використовують протокол ARP. Розроблена модель та метод демонструють виняткову надійність, досягаючи 100% точності виявлення ARP-спуфінгу, що має вирішальне значення для підтримки швидкості реагування мережі. Результати аналізу можуть бути використані для прийняття обґрунтованих рішень щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації. Використання ШІ для моніторингу та аналізу мережевого трафіку дозволяє значно підвищити ефективність і швидкість виявлення загроз. Завдяки здатності адаптуватися до нових типів атак і виявляти складніші шаблони аномалій, запропонований підхід забезпечує більш високий рівень безпеки мережевої інфраструктури. Це дослідження демонструє потенціал інноваційних технологій у боротьбі з кіберзагрозами та сприяє розвитку надійних методів захисту для сучасних мереж.

Ключові слова: аналіз мережевого трафіку, ARP Spoofing, штучний інтелект, атаки на рівні L2

Вступ. Виявлення загроз типу ARP-атак залишається надзвичайно актуальним у сучасному мережевому середовищі. Незважаючи на розвиток технологій безпеки, ARP-атаки продовжують бути ефективними засобами для порушення конфіденційності, цілісності та доступності даних у мережах. Це пояснюється тим, що ARP-протокол, який був розроблений багато років тому, не має вбудованих механізмів захисту, і тому залишається вразливим до підробки та інших форм експлуатації.

Розповсюдження IoT-пристроїв та SDN мереж додатково збільшує поверхню для атак. IoT-пристрої часто мають обмежені можливості для забезпечення безпеки і можуть стати легкою мішенню для зловмисників, які здійснюють ARP-спуфінг. Також

SDN, з його централізованим управлінням мережею, може бути серйозно уражений, якщо атака успішно проведена, що може призвести до значних порушень у мережевій інфраструктурі.

Незважаючи на те, що архітектура SDN виступає як надійна структура, що підвищує безпеку мережі та оптимізує мережеве адміністрування, вона не усуває різні форми атак підробки. Серед них атаки *Distributed Denial of Service* (DDoS) і *Man-in-the-Middle* (MitM) залишаються серйозними загрозами, потенційно скомпрометувавши конфіденційні дані користувачів у мережі. Примітно, що одним із найпоширеніших вторгнень у локальні мережі (LAN) є підробка ARP.

Актуальність виявлення ARP-атак також підсилюється зростаючими вимогами до кібербезпеки у різних секторах, таких як фінанси, охорона здоров'я, промисловість та державні установи. У цих сферах порушення мережевої безпеки може мати серйозні наслідки, включаючи фінансові втрати, втрату конфіденційної інформації та підрив довіри до організації.

Пристрої мережі, які працюють на другому рівні еталонної моделі OSI (*Open Systems Interconnection*) вважаються найслабшою ланкою в інфраструктурі безпеки [1-3, 6]. Розповсюджена IT-політика BYOD (*Bring Your Own Device*), використання віртуальних мереж SDN і низки складних атак, збільшують вірогідність того, що мережі стають більш уразливими до проникнення саме на рівні L2. Протоколи рівня L2 дуже часто залишаються без належної уваги і здебільшого працюють зі стандартною конфігурацією. Слід пам’ятати, що порушення мережної безпеки на рівні L2 також впливатиме на всі рівні, розташовані вище. Таким чином, фахівцям з мережної безпеки потрібно також запобігати і вчасно нейтралізувати атаки на інфраструктуру LAN рівня L2.

Поширена загроза підробки ARP створює значний ризик для безпеки комп’ютерних мереж, що призводить до потенційного підслуховування, фальсифікації та порушення мережевого трафіку. Виявлення ARP-атак є складним завданням, і їх наслідки можуть бути серйозними, включаючи крадіжку даних і вразливість мережі. Ця вразливість у поєднанні з недоліками протоколів ARP відкриває зловмисникам шляхи для використання даних топології мережі, що призводить до різних провалів безпеки.

В роботі проведений аналіз атак, які базуються на маніпулюванні протоколом ARP. Наведено приклади трафіку, який утворюється при активізації атаки з використанням протоколу ARP. Використання методів машинного навчання для виявлення ARP-атак представляє собою інноваційний підхід, який дозволяє підвищити точність і ефективність захисту мереж. Завдяки здатності ML-алгоритмів аналізувати великі обсяги даних у режимі реального часу і виявляти аномалії, сучасні системи захисту можуть більш ефективно ідентифікувати та реагувати на загрози, забезпечуючи більш високий рівень безпеки для мереж різного масштабу і призначення.

Мета даної роботи полягає у підвищенні безпеки виявлення ARP-атак на основі використання методів штучного інтелекту для аналізу мережевого трафіку в режимі реального часу, що включає детальний аналіз ARP протоколів та існуючих методів захисту, оцінку їх обмежень, а також застосування інструментів для збору та аналізу даних, таких як Wireshark. Основною задачею є підвищення точності та швидкості виявлення ARP-спуфінгу, забезпечуючи надійний захист мережевої інфраструктури в умовах зростаючих кіберзагроз, зокрема у середовищах з великою кількістю IoT-пристроїв та SDN мереж.

1. Аналіз та особливості атак на протоколи ARP. ARP – це широко використовуваний протокол, який перетворює IP-адресу на MAC-адресу (*Media Access Control*). В більшості випадків ARP необхідний для того, щоб пристрої могли знаходити один одного в межах одного сегменту мережі. Цей протокол застосовується при організації мереж за протоколом TCP/IP (з використанням протоколу IPv4) для перетворення IP-адреси в MAC-адресу і визначений у стандарті RFC 826. У процесі

перетворення адрес за протоколом ARP застосовуються лише два типи пакетів: ARP-запит та ARP-відповідь. Трафік з використанням протоколу ARP зазвичай виникає в процесі обміну даними по мережі тоді, коли MAC-адреса одержувача невідома. Пристрій, що передає, спочатку шукає цю адресу у своєму кеші. Якщо адреса відсутня в кеші, то вона може бути отримана шляхом додаткового обміну даними по мережі з використанням протоколу ARP. Як тільки процес перетворення адрес завершиться, передавальний пристрій оновить свою кеш-пам'ять і помістить у неї відповідність MAC і IP-адрес приймального пристрою і почне передачу даних. Приклад ARP-таблиці хосту (отримана командою *arp –a*) наведена на рис. 1.

```
PS C:\Users\robst> arp -a

Interface: 192.168.1.246 --- 0x3
  Internet Address      Physical Address      Type
  192.168.1.1           bc-76-c5-1d-19-56     dynamic
  192.168.1.245         f8-ac-65-86-fb-28     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Рис. 1. Приклад ARP-таблиці хосту

Для аналізу мережевого трафіку в режимі реального часу використовувалася платформа *Wireshark* [6], яка є потужним інструментом для виявлення, діагностики та усунення проблем у мережах. Основні призначення *Wireshark* включають захоплення пакетів даних, які проходять через мережу, надання детальної інформації про кожен пакет, діагностування проблем з підключенням, затримками, втратами пакетів, виявлення аномалій та ін. *Wireshark* використовується для виявлення потенційних загроз та аномальної активності в мережі, таких як ARP-атаки, DoS-атаки та інші види зловмисного трафіку. Приклад перехвату типового трафіку між пристроями інструментом *Wireshark* з використанням протоколу ARP наведений на рис. 2.

arp

No.	Time	Source	Destination	Protocol	Length	Info
81…	-35.757171	XiaomiMobile_8d:13:f2	Broadcast	ARP	60	Who has 192.168.31.251? Tell 192.168.31.1
82…	-35.747205	XiaomiMobile_8d:13:f2	Broadcast	ARP	60	Who has 192.168.31.252? Tell 192.168.31.1
83…	-35.737161	XiaomiMobile_8d:13:f2	Broadcast	ARP	60	Who has 192.168.31.253? Tell 192.168.31.1
84…	-35.727217	XiaomiMobile_8d:13:f2	Broadcast	ARP	60	Who has 192.168.31.254? Tell 192.168.31.1
47…	5.953990	XiaomiMobile_8d:13:f2	HewlettPacka_0a:3e:d1	ARP	60	Who has 192.168.31.150? Tell 192.168.31.1
47…	5.954007	HewlettPacka_0a:3e:d1	XiaomiMobile_8d:13:f2	ARP	42	192.168.31.150 is at 84:a9:3e:0a:3e:d1

Рис. 2. Типовий ARP трафік в середовищі Wireshark

З рисунку 2 видно, що ARP-запит посилається в широкомовному режимі (*broadcast message*), а ARP- відповідь надсилається в одноадресному режимі (*unicast message*). Також можливі випадки утворення трафіку, який складається з так званих самочинних ARP-пакетів (ARP-пакети, які генеруються автоматизованими засобами або зловмисниками для порушення нормальної роботи мережі), що також є типовим видом трафіку. Поява самочинних ARP-пакетів можна виявити у ряді випадків:

- зміна IP-адреси пристрою призведе до появи самочинних пакетів;
- при запуску деяких операційних систем відбувається передача самочинних ARP-пакетів;
- в ряді систем самочинні ARP-пакети слугують для підтримки балансування навантаження.

Приклад перехвату трафіку з самочинним ARP-пакетом наведений на рис. 3. З рисунку видно, що самочинні ARP-пакети розсилаються в широкомовному режимі.

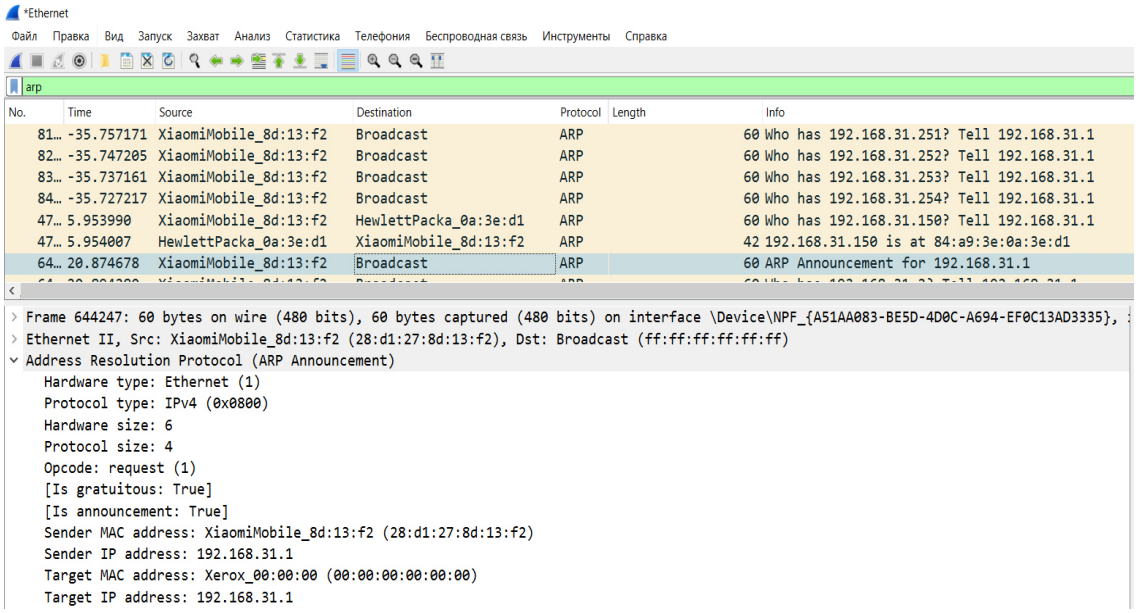


Рис.3. Типовий ARP трафік з самочинним ARP-пакетом

Протокол ARP був стандартизований багато років тому і ніколи не було способу гарантувати автентичність ARP-повідомлення. Як наслідок, є кілька атак ARP, які можуть неправильно спрямувати трафік в локальній мережі з метою його перехоплення в зловмисних цілях. Деякі з атак і методи, які використовуються для проникнення через ARP-протокол, включають:

1. ARP Спуфінг (ARP Spoofing) - є найбільш поширеним типом ARP-атак. Вона полягає у надсиланні фальшивих ARP-повідомлень в мережу для зміни асоціацій між IP-адресами та MAC-адресами. Це дозволяє зловмиснику перенаправляти трафік через свій пристрій. Основні види ARP-спуфінгу включають *Man-in-the-Middle (MITM)* атака та *Packet Sniffing*;

2. ARP Cache Poisoning - атаки передбачають надсилання фальшивих ARP-повідомлень для заповнення ARP-кешу мережевих пристроїв помилковими записами. В результаті цього пакети можуть бути спрямовані на неправильні або неіснуючі MAC-адреси, що призводить до порушення роботи мережі. Види ARP Cache Poisoning включають *Denial of Service (DoS* - перенаправлення трафіку на неіснуючі MAC-адреси, що призводить до неможливості досягти цільового пристрою) та *Network Disruption* (вплив на маршрутизацію трафіку, що призводить до дезорганізації роботи мережі);

3. ARP шторм (Flooding) - зловмисник надсилає велику кількість ARP-запитів або відповідей для перевантаження ARP-кешу мережевих пристроїв. Основні наслідки такої атаки є *Resource Exhaustion* (перевантаження кешу ARP може призвести до сповільнення роботи або навіть збою мережевих пристроїв) та *Network Congestion* (велика кількість ARP-пакетів може перевантажити мережу, зменшуючи її продуктивність);

4. ARP-пінг (ARP Ping) - це метод, який використовується для виявлення активних пристроїв у локальній мережі шляхом надсилання ARP-запитів. Зловмисники можуть використовувати ARP-пінг для збору інформації про пристрої в мережі перед проведенням інших атак.

Атака *ARP spoofing*, також відома як «*отруєння кешу*» *ARP*, використовується в атаці типу «людина посередині» [5, 6]. Під час атаки *ARP spoofing* зловмисник діє наступним чином: надсилає небажане, підроблене повідомлення відповіді *ARP*, яке містить підроблену MAC адресу машини зловмисника для всіх хостів у локальній мережі. Після отримання відповіді *ARP* усі пристрої в локальній мережі оновлять свої *ARP* або таблиці MAC-адрес із неправильною MAC-адресою. Це ефективно *«отруює кеш»* на кінцевих пристроях. Якщо таблиці *ARP* «*отруєні*», це дозволить зловмиснику

видати себе за інший хост, щоб отримати доступ до конфіденційної інформації. Таким чином, трафік спрямовується не на фактичний хост, а на хост із підробленою MAC-адресою. На наведеному нижче рисунку (рис.4) представлена атака ARP, де зловмисник надіслав фальшиву відповідь, яка «*отруїла кеш*» в пристроях. Усі хости в мережі тепер думають, що 10.40.10.103 знаходиться на 46:89:FF:4C:57, замість 00:80:68:B4:87.

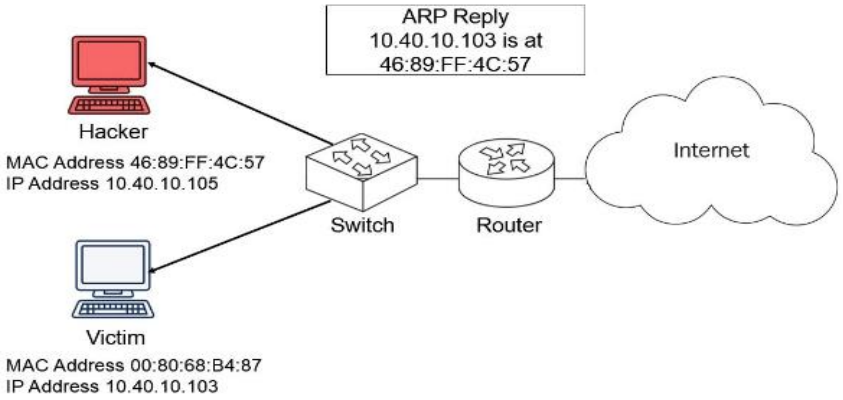


Рис. 4. Атака ARP spoofing

Зазвичай при проведенні атаки, націленої на отруєння кешу ARP, суб'єкт загрози може надсилати іншим хостам у підмережі *самочинні* ARP-відповіді, які містять MAC-адресу зловмисника і IP-адресу шлюзу за замовчуванням. Приклад трафіку, який можна спостерігати при атаці отруєння кешу ARP показано на рис. 5.

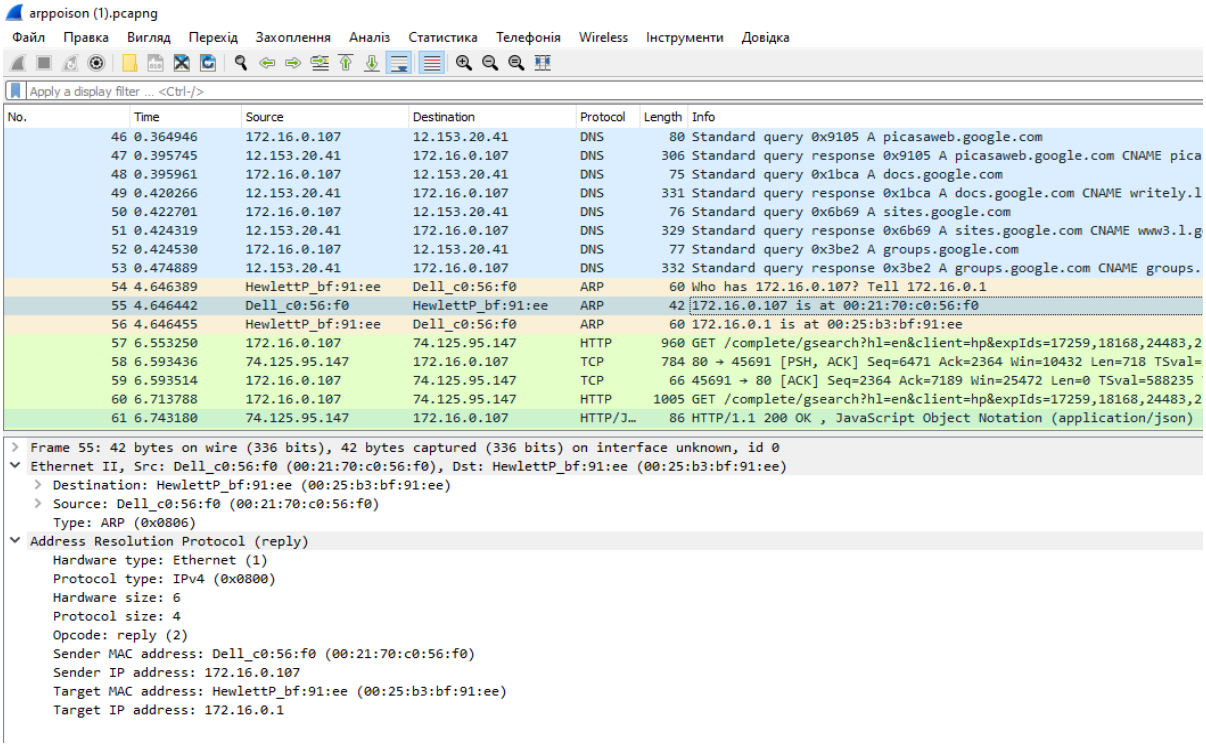


Рис. 5. Приклад трафіку при атаці типу отруєння кешу ARP

З наведеного прикладу видно, що хост зловмисника направляє одноадресний запит і одноадресну відповідь, в яких видає себе за шлюз з IP-адресою 172.16.0.1

Якщо зловмисник перенаправляє трафік, тоді він може перехопити його для отримання конфіденційної інформації, що може стати підготовкою до більш складної атаки.

Шторм ARP (Flooding). У локальній мережі типовим трафіком є ARP-повідомлення запитів/відповідей. При цій атаці можна спостерігати велику кількість ARP-запитів, тому ARP-шторм є формою атаки на відмову в обслуговуванні (DoS).

Для ефективної доставки даних комутатор використовує таблицю *Content Addressable Memory* (CAM), яка містить пари MAC-адрес і пов'язані з ними фізичні порти комутатора. Зловмисник може самовільно надсилати комутатору ARP-повідомлення із підробленою MAC-адресою, в результаті чого комутатор оновлюватиме свою MAC-таблицю. Оскільки всі MAC-таблиці мають обмежений розмір, комутатор може вичерпати ресурси для зберігання MAC-адрес. Атаки з переповнення таблиць MAC-адрес (MAC-флуд), користуючись цим обмеженням, бомбардують комутатор кадрами з підробленими MAC-адресами джерела, допоки таблиця MAC-адрес комутатора не заповниться.

Шторм ARP заповнює таблицю CAM комутатора і переповнює її тисячами фіктивних записів. У цей момент комутатор просто діє як концентратор і надсилає дані на всі порти. Наслідки такої атаки можна охарактеризувати наступним чином:

- у зловмисника з'являється можливість перехоплення всього трафіку з можливим наступним розкриттям конфіденційних даних;
- через велику кількість широкомовних запитів знижується пропускна здатність мережі.

Приклад трафіку, який можна спостерігати при атаці «ARP-шторм», показано на рис.6.

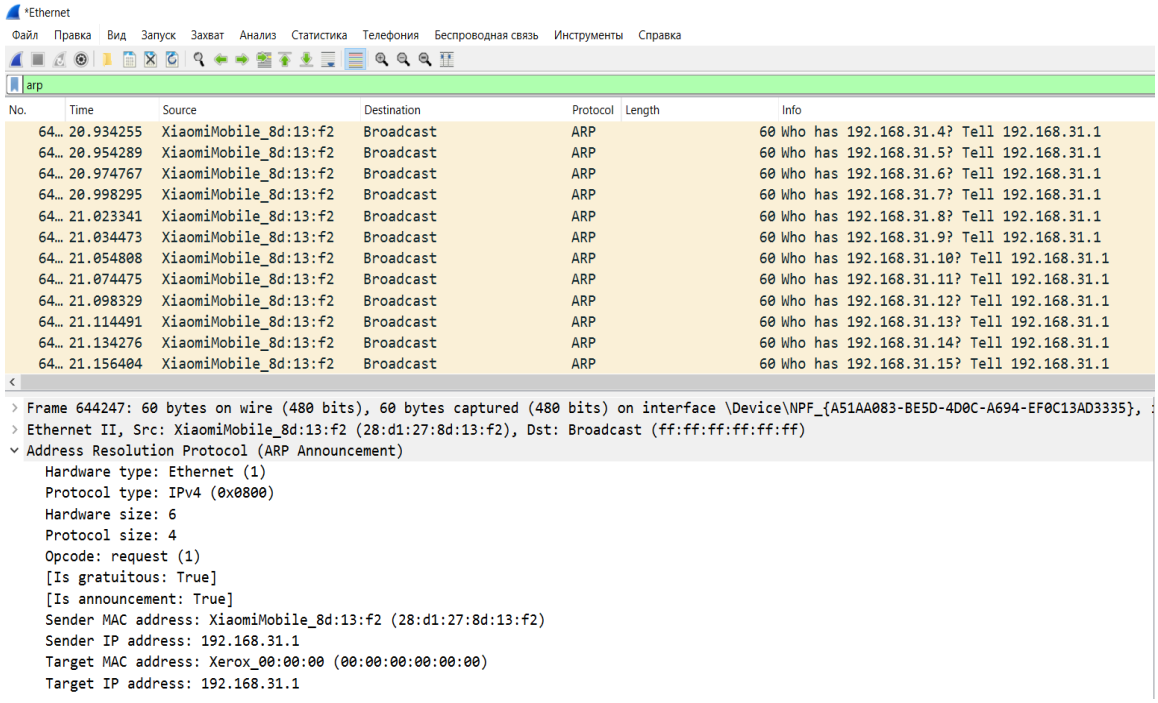


Рис.6. Приклад трафіку при атаці типу ARP-шторм

2. Методи захисту від ARP-атак. Виявлення трафіку, який спричинений атакою *ARP spoofing*, є досить складною операцією, так як потребує аналізу і виявлення шкідливого трафіку при активізації атаки *ARP spoofing* (початковий етап «*отруєння ARP кешу*») і аналізу і виявлення самого факту, що трафік переадресовується через вузол зловмисника. Щоб виявити цю загрозу використовують наступні підходи [5, 6]:

- системи виявлення/запобігання вторгненням (IDS/IPS - *Intrusion Detection Systems/Intrusion Protection Systems*), які налаштовують пристрої для відстеження аномальної активності ARP, наприклад штормів ARP, які зазвичай мають специфічні сигнатури. Пристрій має надіслати сповіщення, якщо буде виявлено небажані відповіді;
- статичні записи ARP - жорстке відображення адрес для запобігання спуфінгу. Це унеможливлює автоматичну актуалізацію ARP-кешу і захищає від підроблених

ARP-повідомлень. Однак цей метод вимагає адміністративних зусиль для підтримки і оновлення Це не найкращий метод, оскільки він погано масштабується у великих мережах;

- брандмауери – використовується лише список контролю доступу з фільтрацією пакетів авторизованого трафіку, який знаходиться в сегменті мережі;
- програмне забезпечення для захисту від ARP - це програмне забезпечення відстежує спуфінг, який може представлятися як дві IP-адреси з однаковою MAC-адресою, а також інші методи для виявлення зловмисної поведінки ARP.

Аналіз літературних джерел доводить, що на основі цих підходів проводяться багатогранні наукові дослідження. У роботі [7] продемонстровано методи щодо протидії атакам ARP-спуфінгу в межах SDN. Їх основною технікою є система виявлення та запобігання вторгненням (*Detection and Prevention System* - IDPS), що використовує технологію SDN. Цей IDPS динамічно адаптує параметри SDN для виявлення та запобігання підозрілим мережевим діям, додаючи до чорного списку шкідливі MAC-адреси. Для персоналізації та оцінки ефективності IDPS було розроблено спеціалізоване програмне забезпечення, інтегроване зі спеціальною бібліотекою для перевірки введених користувачем даних.

В роботі [8] проведене дослідження, спрямоване на боротьбу з обома основними типами ARP-атак у SDN. Запропоноване рішення розширює функціональні можливості контролера SDN шляхом включення спеціального модуля ARP. Цей модуль швидко виявляє та пом’якшує атаки, не перевантажуючи та не спричиняючи відмову в обслуговуванні (DoS) на контролері.

В роботі [9] представлена система, призначена для автономної ідентифікації та протидії мережевим вторгненням, з особливим акцентом на трафік ARP. Використовуючи підхід, заснований на складних обчисленнях, ця система визначає зловмисників або порушників і скасовує доступ до мережі, дозволяючи авторизованим користувачам продовжити роботу. Це підвищує продуктивність системи в таких сферах, як виявлення атак, пом’якшення та оптимізація пропускної здатності. Існують певні обмеження, наприклад, складність обчислень може вплинути на роботу у реальному часі.

В [10] запропоновано механізм, призначений для боротьби з підробкою ARP. Їхня система працює через спеціальну машину, яка співпрацює з контролером SDN для збору інформації про топологію мережі та ARP-запитів. Суть цього підходу полягає в перенаправленні ARP-трафіку на виділену машину, де спеціалізовані методи аналізують дані. Ці та інші методи передбачають наявність спеціального обладнання на базі контролерів SDN або окремих виділених машин, що не завжди може бути реалізованим, в тому числі при розгортанні мереж для пристроїв IoT або ресурсообмежених систем.

Впровадження сучасних методів машинного навчання (ML) для захисту від ARP-атак є актуальною та перспективною стратегією. Серед основних підходів щодо застосування ML відносяться наступні:

1. *Виявлення аномального ARP-трафіку* - моделі машинного навчання можуть бути навчені на основі великого обсягу даних ARP-трафіку для виявлення аномалій, наприклад:
   - *методи класифікації* - використання алгоритмів класифікації, таких як Random Forest, Support Vector Machines (SVM) або нейронні мережі для ідентифікації аномального ARP-трафіку порівняно з нормальним;
   - *кластеризація* - аналіз ARP-повідомлень для виявлення змін, які можуть свідчити про спроби підробки або інші аномалії.

2. *Застосування рішень з машинного навчання на мережевих пристроях* - деякі мережеві пристрої можуть підтримувати вбудовані моделі машинного навчання для моніторингу ARP-трафіку та автоматичного реагування на виявлені загрози, наприклад:

- *мережеві комутатори з DAI* - використання *Dynamic ARP Inspection* (DAI) для перевірки коректності ARP-повідомлень за допомогою навчених моделей;
- *системи виявлення вторгнень (IDS)* - інтеграція з системами IDS, які використовують машинне навчання для виявлення нестандартних патернів ARP-трафіку.

3. *Оновлення моделей і навчання в реальному часі* - враховуючи динамічну природу мережевих атак, важливо мати можливість постійно оновлювати моделі машинного навчання і навчати їх на нових даних. Це дозволяє підтримувати ефективність виявлення навіть у змінних умовах мережі.

Прикладом застосування ML для аналізу мережевого трафіку може бути робота [11], в якій пропонуються алгоритми для виявлення DDoS-атак у межах SDN. В цих алгоритмах використовуються алгоритм *K-means++*, доповнений алгоритмом *Fast k Nearest Neighbor*. Основою цього підходу є модульна система виявлення, яка повністю інтегрована в контролер SDN. Контролер періодично взаємодіє з комутаторами для оцінки та ідентифікації мережевих потоків. Якщо вхідний потік має ознаки DDoS-атаки, контролер негайно налаштовує правила пересилання таблиці потоків і надсилає сповіщення комутатору, організовуючи гнучку відповідь на аномалію. Через періодичну оцінку потоку можуть виникати потенційні накладні витрати на ресурси, що впливає на продуктивність мережі.

В роботі [12, 13] представлено метод штучного інтелекту на основі нейронних мереж для виявлення ARP-спуфінгу в мережах IoT. Запропоновані методи демонструють високу точність у виявленні ARP-спуфінгу в мережах Інтернету речей. Разом з цим необхідно відміти складність розгортання і навчання нейронних мереж, що потребує додаткових ресурсів на отримання моделі ML.

Детальний аналіз різноманітних підходів щодо виявлення ARP атак в мережах наведено в роботі [14], де представлені порівняльні характеристики ефективності різних методів.

3. Архітектура запропонованої моделі ML для аналізу ARP атак в реальному часі

Побудова простого методу машинного навчання для виявлення ARP-атак на локальному комп'ютері або мережі має свої переваги порівняно з застосуванням спеціалізованих контролерів SDN. До таких переваг можна віднести:

- *простота і швидкість впровадження* - простий метод машинного навчання може бути реалізований в короткі строки без значних інвестицій у нове обладнання або програмне забезпечення. Він може використовувати наявні дані і інфраструктуру, що значно спрощує процес впровадження і витрати на підтримку;
- *незалежність від інфраструктури* - метод ML може функціонувати навіть у стандартних мережевих середовищах без необхідності внесення значних змін у існуючу інфраструктуру. Це робить його універсальним і придатним для різних типів мереж та організацій;
- *гнучкість і адаптивність* - методи машинного навчання можуть бути легко адаптовані до нових атак і змін у мережевих умовах через оновлення моделей навчання «на льоту». Це дозволяє швидко реагувати на нові загрози і покращувати точність виявлення аномалій з часом;
- *ефективність в розподілених середовищах* - моделі машинного навчання можуть бути навчені локально на кожному комп'ютері або вузлі мережі, що дозволяє розподілене виявлення загроз без необхідності централізованого керування.

У той час, як спеціалізовані контролери SDN можуть надавати розширені можливості управління та моніторингу мережі, їх впровадження і підтримка можуть бути витратними і складними. Особливо це стосується малих і середніх підприємств, які можуть не мати необхідної інфраструктури або бюджету для впровадження SDN.

Отже, побудова простого та ефективного методу машинного навчання для виявлення ARP-атак може бути доступним рішенням для багатьох організацій,

забезпечуючи необхідний рівень безпеки мережі без значних інвестицій та складнощів, пов'язаних з SDN.

В роботі пропонуються спеціалізовані програмні рішення на мові Python, які базуються на застосуванні моделей машинного навчання, які своєчасно класифікують і виділяють ARP атаки та створюють керуючі сигнали для оповіщення. Розробка та застосування таких моделей *ШІ дозволяє автоматизувати аналіз* мережевого трафіка в реальному часі на основі даних з платформи *Wireshark* та підвищити безпеку комп'ютерних мереж.

На рис.7 наведена загальна структура підготовки даних для побудови моделі ML. Попередня обробка даних є важливою процедурою для забезпечення якості та надійності результатів аналізу даних і роботи моделей машинного навчання. Добре оброблені дані допомагають покращити точність та інтерпретованість моделей, а також зменшити можливість виникнення помилок під час аналізу. Для отримання моделі ML, яка буде завантажуватися і використовуватися для аналізу даних в реальному часі, потрібно виконати декілька підготовчих етапів.

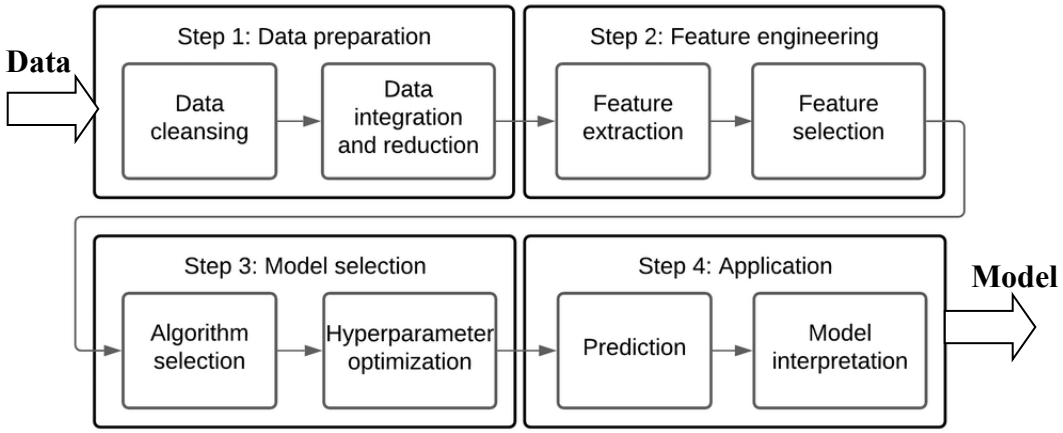


Рис.7. Загальна структура підготовки даних для побудови моделі ML.

Підготовка даних (Step 1). Це перший крок, де данні (Data) можуть збиратися з різних джерел, зокрема, в даній роботі – з платформи *Wireshark.* На основі збереженого трафіку у форматі *.CSV* формується DataFrame. Якщо такий DataFrame не містить ARP атак, тоді до нього додаються нові записи, які характерні для відповідних ARP атак. На цьому етапі відбувається очищення даних (Data Cleaning), видаляються або коригуються неправильні, відсутні або непотрібні дані (Missing value), відбувається фільтрація ARP-пакетів і залишаються тільки ті, які належать до протоколу ARP.

Конструювання ознак (Step 2). На цьому етапі відбувається вилучення зайвих ознак (*Feature Extraction*) і виділення необхідних (*Feature Selection*), в тому числі можуть створюватися нові. Якщо датасет містить багато ознак, які не є важливими для аналізу або моделювання, вони можуть бути видалені, щоб спростити аналіз, зменшити розмірність та обчислювальні витрати. Даний етап реалізується різноманітними методами аналізу даних, в тому числі кореляційними підходами.

Вибір і підготовка моделі (Step 3). На цьому етапі відбувається кодування категоріальних ознак (*Encoding Categorical Features*) для переведення їх в числовий формат, масштабування ознак (*Feature Scaling*) для забезпечення однакового діапазону значень і покращення швидкості навчання моделей. Окрім того, на цьому етапі відбувається вибір алгоритму (класифікатора) для побудови моделі та визначення оптимальних гіперпараметрів.

Останній етап (Step 4) призначений для формування моделі ML, збереження цієї моделі або декількох в залежності від потреб аналізу атак. Отримані моделі

використовуються для прогнозування різноманітних атак, на які вони були налаштовані та навчані.

На рис.8 представлений промаркований DataFrame на основі реальних даних, отриманих з платформи *Wireshark.* Як видно з даних, записи #56, #168 представляють *ARP spoofing* і вони, відповідно, промарковані як аномальні, де Out = «1». Якщо під час аналізу трафіку не було аномальних записів, то їх можна синтетично додати, створивши таким чином власний промаркований DataFrame з бажаним видами атак, які потрібно розпізнати.

No.	Time	Source	Destination	Protocol	Length	Info	Out
324	9.021666	72:7e:18:e7:d2:ef	Broadcast	ARP	60	Gratuitous ARP for 192.168.119.80 (Request)	0
54	4.646389	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60	Who has 172.16.0.107? Tell 172.16.0.1	0
55	4.646442	Dell_c0:56:f0	HewlettP_bf:91:ee	ARP	42	172.16.0.107 is at 00:21:70:c0:56:f0	0
56	4.646455	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60	172.16.0.1 is at 00:25:b3:bf:91:ee	1
166	6.744431	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	50	Who has 172.18.10.10? Tell 172.16.0.5	0
167	6.748552	Dell_c0:56:f0	HewlettP_bf:91:ee	ARP	88	172.18.10.10 is at 01:2f:20:ce:44:fa	0
168	6.750123	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	50	172.16.0.5 is at 34:56:af:31:9f:26	1
165	14.392559	HewlettP_bf:91:ee	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.105	0
166	4.646389	HewlettP_bf:91:ee	Dell_c0:56:f0	ARP	60	Who has 172.16.1.108? Tell 172.16.0.2	0

Рис.8. Сформований DataFrame на базі трафіку платформи *Wireshark.*

Отриманий DataFrame необхідно трансформувати в такий вид, щоб він був придатний для отримання моделі ML. В роботі пропонується модель на основі ключових ознак «Source», «Destination», «Info» та «Out», де «Out» - марковані мітки, які відповідають нормальному («0») і аномальному («1») трафіку.

В роботі розглядається задача побудови простої і ефективної моделі класифікації трафіка, тому застосовувалися класичні класифікатори ML, вбудовані до бібіліотеки *Sklearn Python*. Окрім того, при отриманні моделі класифікації потрібно враховувати часові залежності надходження пакетів, щоб не застосовувати складні нейромережеві структури типу LSTM *(Long Short-Term Memory*) та ін. Для цього запропоновано ряд функцій для побудови моделі формування нового DataFrame, придатного для застосування в ML:

- *ip_to_int(ip)* - приймає IP-адресу як рядок і повертає її числовий еквівалент. Якщо IP-адреса порожня або дорівнює '0.0.0.0', функція повертає 0;
- *mac_to_int(mac)* приймає MAC-адресу як рядок і повертає її числовий еквівалент. Якщо MAC-адреса порожня або дорівнює '00:00:00:00:00:00', функція повертає 0. Функція також замінює шістнадцяткові літери на відповідні числові значення перед обчисленням;
- використовуються регулярні вирази для аналізу IP- та MAC-адрес, додаються нові ознаки, такі як «who_has», «ip1», «tell», «ip2», «is_at», «ip_at», «mac», які містять відповідні частини ARP-пакетів;
- текстові частини, такі як «who_has», «tell», «is_at», кодуються у числовий формат за допомогою *LabelEncoder* для подальшого використання в алгоритмах ML;
- формується новий DataFrame з результатами для зберігання закодованих і числових значень;
- обробка пакетів відбувається циклічно по всіх рядках початкового DataFrame, аналізуючи відповідність «who_has», «tell», «is_at» ознаки «Info».

Результатом такої підготовки даних є новий DataFrame, представлений на рис.9. В ньому міститься перетворена інформація ключових ознак (рис.8), які можуть бути використані для побудови моделі ML (Step 3).

	who_has_encoded	ip1_int	tell_encoded	ip2_int	is_at_encoded	ip_at_int	mac_int	Label
0	0	0	0	0	0	0	0	0
1	1	2886729835	1	2886729729	1	2886729835	91376597142	0
2	0	0	0	0	1	2886729729	109343105158	1
3	1	2886863370	1	2886729733	1	2886863370	2023344714214	0
4	0	0	0	0	1	2886729733	37640944653082	1
...	...	...	...	...	...	...	...	...
210	1	3232235683	1	3232235550	0	0	0	0
211	1	3232235684	1	3232235550	0	0	0	0
212	1	2886731216	1	2886729985	1	2886731216	108573441259	0
213	0	0	0	0	1	2886729985	1115297164974881	1

Рис.9. Сформований DataFrame за результатом виконання конструювання ознак.

Для отримання моделей ML вхідні дані мережевого тарфіка (*Network Traffic*) утворюють Dataset, який підлягає попередній обробці (*Preprocessing*) згідно загальної структури на рис.7. Такий набір данних був розділений на тренувальний (*Train Data* - 70%) і тестовий (*Test Data* - 30%) набори (рис.10). Тренувальний набір використовується для отримання моделі класифікації для різних класифікаторів. В роботі було застосовано декілька класичних і добре відомих класифікаторів ML бібліотеки Sklearn, зокрема *DecisionTreeClassifier, LogisticRegression, SVM.* Навчані моделі були збережені для подальшого виклику і розгортання у форматі *.PKL*. Таким чином, для аналізу трафіку в реальному часі в подальшому відпадає необхідність поточного навчання моделі і витрата ресурсів і часу, що може бути досить вагомим аргументом для ресурсообмежених систем та мереж. Замість цього можна скористатися заздалегідь підготовленим набором моделей або їх комбінаціями в залежності від поставленої задачі.

Тестовий набір даних (*Test Data*) використовується для валідації якості отриманих моделей по ряду показників ефективності. Таким показниками слугують відомі характеристики: якість (*Accuracy*), влучність (*Precision*), повнота (*Recall*), *f1*-оцінка. Всі показники ефективності на тестовому наборі для вказаних класифікаторів показали максимальний результат – *1.0*, тобто сто відсоткову відповідність при менших часових ресурсах на навчання моделі у порівнянні із застосуванням нейромережевих моделей.

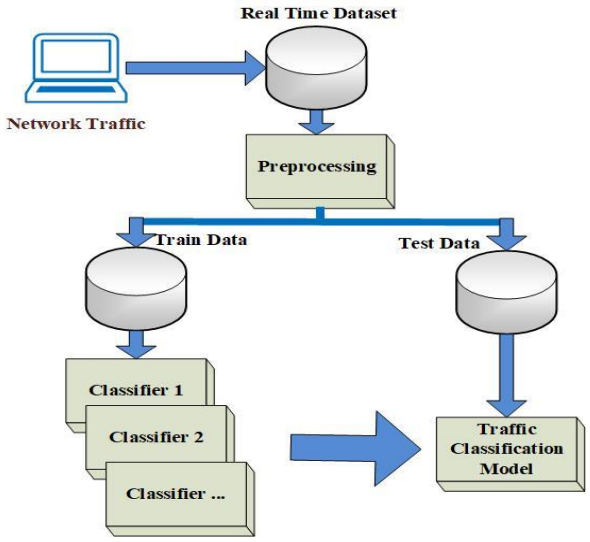


Рис.10. Модель побудови класифікаторів і валідації їх ефективності

Подальше вдосконалення моделей залежить від гіперпараметризації - налаштування гіперпараметрів моделі для досягнення найкращих результатів. При

потребі дані моделі можуть вдосконалюватися і підналаштовуватися під інші види мережевих атак без зміни апаратної частини і застосування коштовних контролерів SDN.

Серед останніх етапів виділяються наступні:

- впровадження моделі - перенесення навченої моделі в виробниче середовище для використання в реальних умовах згідно трафіку, отриманого з платформи *Wireshark;*
- моніторинг та підтримка - слідкування за продуктивністю моделі в реальному часі та оновлення її при необхідності.

4. Результати дослідження та обговорення. Впровадження отриманої моделі аналізу мережевого трафіка для аналізу ARP атак потребує розробки *системи автоматизованої підтримки* перетворення файлів .PCAPNG, які формує платформа *Wireshark* в режимі реального часу у формат .CSV. *Wireshark* має налаштування щодо формування файлів .PCAPNG заданих розмірів для їх подальшого збереження. Разом з тим *Wireshark* не передбачає можливості перетворення «на льоту» файлів у формат .CSV, що вимагає розробки додаткового методу автоматизованого перетворення. Отримані «на льоту» .CSV файли потребують попередньої підготовки, щоб до них можна було застосувати попередньо отриману модель ML для класифікації трафіка.

Система *автоматизованої підтримки ML моделі* складається з застосування декількох нових методів.

1. Метод перетворення .PCAPNG файлів платформи *Wireshark* у формат .CSV в режимі реального часу, який полягає в наступному:

- підготовка середовища - визначаються шляхи до папок з вхідними файлами .PCAPNG та вихідними файлами .CSV;
- визначається файл .CSV, який буде виключено з обробки (для усунення некоректної роботи у разі відсутності у трафіку ARP пакетів);
- аналіз пакетів – функція читає вхідний .PCAPNG файл та аналізує пакети для виявлення різних типів протоколів (Ethernet, ARP, IP, DHCP);
- збирання інформації про кожен пакет (джерело, призначення, тип протоколу, довжина та інші деталі);
- запис зібраної інформацію у вихідний .CSV файл.

Основні операції даного методу полягають у:

- отриманні списку всіх .PCAPNG файлів у папці з вхідними файлами (автоматично завантажуються з платформи *Wireshark*);
- визначення, які файли ще не були оброблені;
- циклічно перевіряє папку на наявність нових файлів, які автоматично записуються;
- для кожного нового файлу .PCAPNG викликається функція обробки та збереження результатів у новий .CSV файл;
- додає оброблені файли до списку оброблених, щоб уникнути повторної обробки;
- видаляє файл після обробки, якщо це не виключений файл (щоб не було перевантаження памяті).

2. Метод обробки DataFrame .CSV файла і формування заданих фітчів (ознак) для застосування підготовленої моделі ML, який полягає в наступному:

- фільтрація та вибір даних ARP - обирається підмножина даних, яка містить лише пакети з протоколом ARP;
- обробка текстових даних з ознакою «Info» – текст виділяється на окремі частини за допомогою регулярних виразів для отримання IP-адрес, MAC-адрес та інших даних;
- застосування функцій перетворення даних у числовий формат: IP-адресу та MAC-адресу;
- створення нового DataFrame для зберігання результатів нових перетворень;
- кодування текстових ознак у числові;

- заповнення та структурування результатів перетворення, які за своєю структурою повинні збігатися зі структурою, яка була використана для отримання відповідної моделі ML (рис.9);

Отже, цей метод дозволяє виконати обробку і трансформацію даних .CSV файла для подальшого машинного навчання і застосування підготовленої моделі ML.

3. Аналіз трафіка в режимі онлайн із застосуванням підготовленої моделі ML, який полягає в наступному:

- зчитуються дані з .CSV файлу (формуються на попереньому етапі) і до них додаються інші дані з підготовленого файлу addata.csv на той випадок, якщо у поточному трафіку відсутні APR запити для нормальної роботи моделі ML;
- завантажується підготовлена модель ML для прогнозування класу аномальності і застосовується для кожного окремого підготовленого .CSV файлу;
- виводяться кількісні характеристики аномального трафіку у кожному поточному файлі на екран з подачею звукового повідомлення чи передачею інформації на електронну пошту (при потребі).

Результат обробки файлів у випадку ARP атаки виводиться на екран (електронну пошту, сервер і т.п.) із позначенням номера пакета, який підпадає під атаку (рис.11).

```
File: 1   Number of abnormal traffic - 104
File: 2   Number of abnormal traffic - 203

 Completion of processing files in the directory
```

Рис.11. Результат повідомлення про аномальний трафік

Використання нових моделей машинного навчання для аналізу мережевого трафіку виявилося результативним у практичному застосуванні. Моделі дозволяють ефективно виявляти аномальний трафік у великих обсягах даних в реальному часі, що є критичним аспектом для забезпечення кібербезпеки в сучасних мережах. Основні переваги включають високу точність прогнозування аномальних подій, гнучкість у роботі з різноманітними форматами даних та ефективність у використанні ресурсів обчислювальних систем.

У порівнянні з нейромережевими моделями, які відомі своєю здатністю до автоматичного визначення складних зв'язків у даних, нова модель має певні переваги, які полягають у менших обчислювальних ресурсах для тренування та прогнозування, що робить її більш доступною для впровадження в системах з обмеженими ресурсами, наприклад IoT мережах без застосування складних контролерів SDN. Окрім того, отримані моделі зазвичай володіють більшою інтерпретованістю результатів, що дозволяє оперативно реагувати на виявлені аномалії та виправляти їх.

Впровадження автоматизованої системи аналізу трафіку мережі на базі запропонованих методів обробки даних та нових моделей машинного навчання є перспективним кроком у забезпеченні кібербезпеки та ефективного управління мережевими ресурсами, яке полягає у спрощенні реалізації, збільшенні ефективності та зниженні витрат, що робить її привабливим вибором для сучасних інформаційних технологій.

Висновки. Широке розповсюдження SDN та IoT мереж забезпечило високу гнучкість і ефективність керування ними, але водночас поставило нові виклики у захисті мережевої інфраструктури. Однією з важливих загроз залишаються атаки підробки протоколу розпізнавання адрес - ARP, що порушують цілісність мережі та конфіденційність даних. У цій роботі представлено новий підхід до виявлення ARP-спуфінгу в мережах, який враховує обмеження існуючих методологій і використовує методи машинного навчання ML для аналізу мережевого трафіку в реальному часі. Запропонований метод використовує дані, отримані з платформи Wireshark, і на основі машинного навчання класифікує та виявляє зловмисний мережевий трафік, що виникає

в результаті ARP-атак. Модель демонструє виняткову надійність, досягаючи 100% точності виявлення ARP-спуфінгу, що є критично важливим для підтримки швидкості реагування мережі. Використання методів ML дозволяє значно підвищити ефективність і швидкість виявлення загроз, забезпечуючи високий рівень безпеки мережевої інфраструктури. У порівнянні з нейромережевими моделями, метод машинного навчання має кілька переваг. Він вимагає менше обчислювальних ресурсів для тренування та прогнозування, що робить його доступнішим для впровадження в умовах обмежених ресурсів. Крім того, нова модель є більш інтерпретованою, що дозволяє оперативно реагувати на виявлені аномалії. Простота і швидкість впровадження, незалежність від інфраструктури, гнучкість та адаптивність до нових атак роблять цей підхід привабливим для широкого спектра організацій. Побудова моделі ML для виявлення ARP-атак на локальному комп'ютері також має свої переваги порівняно із застосуванням спеціалізованих контролерів SDN. Вона є ефективною в розподілених середовищах, де моделі можуть бути навчені локально на кожному комп'ютері або вузлі мережі, що дозволяє розподілене виявлення загроз без необхідності централізованого керування. Такий підхід забезпечує необхідний рівень безпеки мережі без значних інвестицій і складнощів, пов'язаних з SDN, що робить його доступним рішенням для багатьох організацій.

Список літератури

1. Odom W.: CCNA 200-301 Official Cert Guide. Volume 1-2. Cisco Press, 2019. 1095 p.
2. Carthern C., Wilson W., Bedwell R., Rivera N. Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Apress Media, 2015. 839 p.
3. Santos O, Stuppi J. CCNA Security 210-260 Official Cert Guide. Apress Media, 2016. 608 p.
4. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В.. Комп'ютерні мережі. Львів: Магнолія 2006, 2013. 256 с.
5. Sanders C. Practical packet analysis. Using Wireshark to solve real-world network problems. 2019. 448 p.
6. Bock L. A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark. 2022. 606 p.
7. Girdler T., Vassilakis V.G.: Implementing an intrusion detection and prevention system using software-defined networking. Defending against ARP spoofing attacks and blacklisted MAC addresses *Comput. Electr. Eng.*, V. 90. 2021. DOI: 10.1016/j.compeleceng.2021.106990
8. AbdelSalam A.M., El-Sisi A.B.V., Reddy K. Mitigating ARP spoofing attacks in software-defined networks. *25th International Conference on Computer Theory and Applications, ICCTA*. 2015. P.. 126-131. DOI: 10.1109/ICCTA37466.2015.9513433
9. Amin R., Hussain M., Alhameed M., Raza S.M., Jeribi F., Tahir A.: Edge-computing with graph computation: A novel mechanism to handle network intrusion and address spoofing in SDN *Comput. Mater. Continua*. V.65 (3). 2020. P. 1869-1890. DOI: 10.32604/cmc.2020.011758
10. Aldabbas H., Amin R.: A novel mechanism to handle address spoofing attacks in SDN based IoT. *Cluster Comput.* V. 24 (4). 2021. P. 3011-3026. DOI: 10.1007/s10586-021-03309-0
11. Xu Y., Sun H., Xiang F., Sun Z.: Efficient ddos detection based on K-FKNN in software defined networks. *IEEE Access.* V. 7. 2019. P. 160536-160545. DOI: 10.1109/ACCESS.2019.2950945
12. Abdulla H., Al-Raweshidy H., Awad W. ARP Spoofing Detection for IoT Networks Using Neural Networks. *Proceedings of the Industrial Revolution & Business Management: 11th Annual PwR Doctoral Symposium (PWRDS*). 2020.
13. Shilpa P. Khedkar, Ramalingam A.C. Classification and Analysis of Malicious Traffic with Multi-layer Perceptron Model. *Ingénierie des Systèmes d'Information.* V. 26. No. 3. P. 303-310. 2021.
14. Hnamte V., Hussain J. Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation. *Telematics and Informatics Reports*, V. 14. 2024.

DEVELOPMENT OF AN ARTIFICIAL INTELLIGENCE METHOD FOR ANALYSIS OF HARMFUL NETWORK TRAFFIC AT CHANNEL LEVEL (ARP ATTACKS)

V.V. Palahin[1], O.A. Palahina[2], O.V. Ivchenko[3], O.M. Panasko[4], R.L. Ptashkin[5]

[1-4]Cherkasy State Technological University
460, Shevchenko blvd., Cherkasy, Ukraine, 18005
[5]Cherkasy scientific research forensic centre MIA of Ukraine
104, Pasterivska st., Cherkasy, Ukraine, 18000
emails: palahin@ukr.net[1], palahina@ukr.net[2],
sania_ivchenko@ukr.net[3] , lena.pa@ukr.net[4], ndekc.ck@gmail.com[5]

The widespread distribution of software-defined networks (Software-Defined Networking - SDN) and IoT networks has provided flexibility and efficiency in network management. However, it has also posed new challenges in protecting network infrastructure. Address Resolution Protocol (ARP) spoofing attacks, which violate network integrity and data confidentiality, remain one of the significant threats. This manuscript presents a new approach to detecting ARP spoofing in networks, addressing the limitations of existing methodologies. The analysis of ARP protocols, their purposes, and basic methods of protection against attacks was carried out. Typical threats to computer networks at the physical and data link layers of the OSI model are presented, along with an analysis of the features of detecting such threats using artificial intelligence (AI) methods. The application of machine learning (ML) methods for traffic analysis based on real-time data from the Wireshark platform is proposed. The new method uses AI to classify and detect malicious network traffic generated by ARP protocol attacks. The developed model and method demonstrate exceptional robustness, achieving 100% ARP spoofing detection accuracy, which is critical for maintaining network responsiveness. The analysis results can be used to make informed decisions about the choice of protection methods for networks with different purposes and information protection requirements. Using AI to monitor and analyze network traffic can significantly increase the effectiveness and speed of threat detection. Due to its ability to adapt to new types of attacks and detect more complex anomaly patterns, the proposed approach provides a higher level of network infrastructure security. This research demonstrates the potential of innovative technologies in the fight against cyber threats and contributes to the development of reliable protection methods for modern networks.
Keywords: network traffic analysis, ARP Spoofing, Artificial Intelligence, L2 Level Attacks

DOI 10.15276/imms.v14.no1-2.85
УДК 519.972.5:004.942.001.57

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 85-96

ПАРАМЕТРИ МЕТОДУ РУНГЕ-КУТТИ З РІЗНИМ ПОРЯДКОМ ТОЧНОСТІ ПРИ ІНТЕГРУВАННІ РІВНЯНЬ ДИНАМІКИ В ЗАДАЧАХ МОДЕЛЮВАННЯ НЕСТАЦІОНАРНИХ СИСТЕМ

С. А. Положаєнко, А. Ю. Прокофьєв

Національний університет «Одеська політехніка»,
1, Шевченка, пр., м.Одеса, 65044, Україна;
emails: sanp277@gmail.com, fallbrick@gmail.com

При створенні та дослідженнях систем моделювання, управління та ідентифікації вкрай важливими етапами є складання та числове розв'язування рівнянь математичних моделей цих систем, які, зазвичай, представляються в класах диференціальних та інтегральних рівнянь. При цьому вирішальними виявляються питання розробки та дослідження обчислювальних алгоритмів, що реалізують методи числового розв'язування рівнянь математичних моделей систем, зокрема, забезпечення контролю показників точності шуканого розв'язку, а також оцінки впливу відхилень параметрів динамічних систем на їх рух та показники якості. Як при аналізі точності числового дослідження математичних моделей динамічних систем, так і при розв'язуванні задач синтезу останніх на основі умов точності, важливе значення має можливість аналітичного вираження додаткового руху збудженої системи. Математичні моделі нестаціонарних систем, представлені у вигляді диференціальних рівнянь у повних похідних, реалізуються, у переважній більшості прикладних задач, методом Рунге-Кутти різних порядків. Показано, що підвищення продуктивності машинного обрахунку при цьому може бути досягнуто у тому випадку, коли вдається врахувати різницю у швидкості зміни різних груп координат досліджуваної нестаціонарної системи. Виконано постановку та розглянуто можливість раціонального вибору параметрів формул методу Рунге-Кутти, що дозволяє мінімізувати час інтегрування рівнянь математичної моделі системи.

Ключові слова*:* нестаціонарна система, математична модель, числовий метод, метод Рунге-Кутти, порядок методу, точність розв'язку.

Вступ. В нестаціонарних системах, динаміка яких описується звичайними диференційними рівняннями наступного виду

$$\frac{d\mathbf{Y}}{dt} = f\left(t, \mathbf{Y}, \mathbf{P}\right), \tag{1}$$

$$Y_i\left(t_s\right) = P_i \ \left(i = \overline{1, l}\right), \tag{2}$$

$$v \in R_v\left(v\right); v \in \left\{t, \mathbf{Y}, \mathbf{P}\right\}, \tag{3}$$

де $\mathbf{Y}\left(t\right)$ — l -мірний вектор вихідного сигналу нестаціонарної системи, $\mathbf{P}\left(v\right)$ — m -мірний вектор параметрів нестаціонарної системи, $R_v\left(v\right)$ — області завдання змінних $v = \left\{\mathbf{Y}, \mathbf{P}\right\}$, t — незалежний аргумент часу.

як правило, можна виділити декілька груп координат з різними швидкостями зміни та з різко відмінними залежностями координат від аргументу, наприклад, з аперіодичним рухом в одній групі та гармонійним або релаксаційним коливанням — у іншій групі. В якості прикладу можна назвати такі координати, як висота та швидкість літального апарату, які повільно змінюються у порівнянні з кутовими швидкостями обертання навколо центру мас літального апарату і які, у свою чергу, повільно

змінюються у порівнянні зі змінними, що описують динаміку приводів керма напрямків, висоти і елеронів.

Очевидно, що для забезпечення бажаної точності моделювання динаміки таких систем необхідно ці групи змінних інтегрувати з різним кроком. Природно при цьому використати числовий метод, який дозволяє легко регулювати крок інтегрування в залежності від швидкостей зміни змінних у відповідній групі координат. Останній вимозі відповідає метод Рунге-Кутти [1 — 4]. Для забезпечення необхідної точності при прийнятних часових витратах на моделювання руху досліджуваної системи з використанням методу Рунге-Куттиє є можливість управляти такими факторами, як *порядок* та *параметри* методу [5]. Конкретизуємо цю можливість за наявної інформації, яку отримано в результаті попередніх досліджень нестаціонарної системи про порядки методу Рунге-Кутти, які забезпечують необхідну точність моделювання відповідної групи рівнянь динаміки.

Мета роботи. Метою роботи є отримання аналітичних виразів, які дають змогу обчислити необхідні порядки методу Рунге-Кутти при розбитті координат досліджуваної системи на групи за швидкістю, що зумовлює визначення кроку інтегрування та забезпечує необхідну точність шуканого розв'язку.

Основна частина. Нехай рівняння досліджуваної нестаціонарної системи розбито по групах координат таким чином, що для кожної наступної групи необхідно збільшення порядку методу. Отримаємо співвідношення для параметрів методу Рунге-Кутти у даному випадку.

Спочатку розглянемо систему, в якій кожну групу параметрів ($g(x), q(x), u(x), w(x)$ — параметри нестаціонарної системи, x — незалежна просторова координата) представлено одним рівнянням:

$$\left.\begin{aligned} \frac{dg}{dx} &= b(x,g,q,u,w);\ g(x_0) = g_0, \\ \frac{dq}{dx} &= c(x,g,q,u,w);\ q(x_0) = q_0, \\ \frac{du}{dx} &= d(x,g,q,u,w);\ u(x_0) = u_0, \\ \frac{dg}{dx} &= h(x,g,q,u,w);\ w(x_0) = w_0. \end{aligned}\right\} \tag{4}$$

Нехай числовий розв'язок системи (4) отримується достатньо точним при використанні методу Рунге-Кутти першого, другого, третього та четвертого порядків для змінних $g(x), q(x), u(x), w(x)$, відповідно. За уяви відповідної гладкості розв'язку системи (4) можемо записати наступні вирази для приростів функцій $g(x), q(x), u(x), w(x)$ на інтервалі $[x_i, x_{i+1}]$:

$$\left.\begin{aligned} \Delta g_i &= g(x_i + s) - g(x_i) = g' \cdot s + O(s^2), \\ \Delta q_i &= q(x_i + s) - q(x_i) = q' \cdot s + \frac{s}{2} q'' + O(s^3), \\ \Delta u_i &= u(x_i + s) - u(x_i) = q' \cdot s + \frac{s^2}{2} q'' + \frac{s^3}{6} u''' + O(s^4), \\ \Delta w_i &= w(x_i + s) - w(x_i) = w' \cdot s + \frac{s^2}{2} w'' + \frac{s^3}{6} w''' + \frac{s^4}{24} w^{(4)} + O(s^5). \end{aligned}\right\} \tag{5}$$

Розрахункові приріст розв'язку системи (4) на інтервалі $[x_i, x_{i+1}]$ відшукуються у вигляді [5, 6]

$$\left.\begin{aligned}\Delta g &= a_{11}\cdot n_1,\\ \Delta q &= e_{21}\cdot m_1 + e_{22}\cdot m_2,\\ \Delta u &= s_{31}\cdot \lambda_1 + s_{32}\cdot \lambda_2 + s_{33}\cdot \lambda_{31},\\ \Delta w &= p_{41}\cdot k_1 + p_{42}\cdot k_2 + p_{43}\cdot k_3 + p_{44}\cdot k_4,\end{aligned}\right\} \tag{6}$$

де

$$n_1 = sb_i = sb\left(x_i, g_i, q_i, u_i, w_i\right), \tag{7}$$

$$\left.\begin{aligned}m_1 &= sc_i = sc\left(x_i, g_i, q_i, u_i, w_i\right),\\ m_2 &= sc\left(x_i + \alpha_2 s, g_i + \xi_{21} n_1, q_i + \delta_{21} m_1, u_i + \gamma_{21}\lambda_1, w_i + \beta_{21} k_1\right),\end{aligned}\right\} \tag{8}$$

$$\left.\begin{aligned}\lambda_1 &= sd_i = sd\left(x_i, g_i, q_i, u_i, w_i\right),\\ \lambda_2 &= sd\left(x_i + \alpha_2 s, g_i + \xi_{21} n_1, q_i + \delta_{21} m_1, u_i + \gamma_{21}\lambda_1, w_i + \beta_{21} k_1\right),\\ \lambda_3 &= sd\left(x_i + \alpha_3 s, g_i + \xi_{31} n_1, q_i + \sum_{j=1}^{2}\delta_{3j} m_j, u_i + \sum_{j=1}^{2}\gamma_{3j}\lambda_j, w_i + \sum_{j=1}^{2}\beta_{3j} k_j\right),\end{aligned}\right\} \tag{9}$$

$$\left.\begin{aligned}k_1 &= sf_i = sf\left(x_i, g_i, q_i, u_i, w_i\right),\\ k_2 &= sh\left(x_i + \alpha_2 s, g_i + \xi_{21} n_1, q_i + \delta_{21} m_1, u_i + \gamma_{21}\lambda_1, w_i + \beta_{21} k_1\right),\\ k_3 &= sh\left(x_i + \alpha_3 s, g_i + \xi_{31} n_1, q_i + \sum_{j=1}^{2}\delta_{3j} m_j, u_i + \sum_{j=1}^{2}\gamma_{3j}\lambda_j, w_i + \sum_{j=1}^{2}\beta_{3j} k_j\right),\\ k_4 &= sh\left(x_i + \alpha_4 s, g_i + \xi_{41} n_1, q_i + \sum_{j=1}^{3}\delta_{4j} m_j, u_i + \sum_{j=1}^{3}\gamma_{4j}\lambda_j, w_i + \sum_{j=1}^{3}\beta_{4j} k_j\right).\end{aligned}\right\} \tag{10}$$

Відповідно до методу Рунге-Кутти параметри розрахункових формул (6) — (10) визначаються з умов:

$$\begin{aligned}&\Delta\varpi_i - \varpi = O\left(s^{\sigma_\varpi}\right),\\ &\varpi \in \{g, q, u, w\},\ \sigma_\varpi \in \{2, 3, 4, 5\}.\end{aligned} \tag{11}$$

Дотримуючись [6], будемо використовувати оператор диференціювання:

$$D_\sigma[\varpi] = \left(\frac{\partial}{\partial x} + b\frac{\partial}{\partial g} + c\frac{\partial}{\partial q} + d\frac{\partial}{\partial u} + h\frac{\partial}{\partial w}\right)^{\sigma}[\varpi]. \tag{12}$$

Позначивши

$$\left.\begin{aligned}\boldsymbol{\Theta} &= \left(\Theta_1, \Theta_2, \Theta_3, \Theta_4\right)^{\mathrm{T}} = \left(g, q, u, w\right)^{\mathrm{T}},\\ \mathbf{F} &= \left(F_1, F_2, F_3, F_4\right)^{\mathrm{T}} = \left(b, s, d, h\right)^{\mathrm{T}},\end{aligned}\right\} \tag{13}$$

в силу системи (4) можемо записати:

$$\left.\begin{aligned}
\frac{d\Theta_j}{dx} &= F_j(x,\boldsymbol{\Theta});\ j=\overline{1,4},\\
\frac{d^2\Theta_j}{dx^2} &= D_1[F_j];\ j=\overline{1,4},\\
\frac{d^3\Theta_j}{dx^3} &= D_2[F_j]+\sum_{\kappa=1}^{n} D_1[F_j]\cdot\frac{\partial F_j}{\partial\Theta_\kappa};\ j=\overline{1,4},\\
\frac{d^4\Theta_j}{dx^4} &= D3[F_j]+\sum_{\kappa=1}^{n}\{3\cdot D_1[F_\kappa]\cdot D_1\left[\frac{\partial F_j}{\partial\Theta_\kappa}\right]+\\
&+ D_2[F_\kappa]\cdot\frac{\partial F_j}{\partial\Theta_\kappa}+D_1[F_\kappa]\cdot\sum_{\eta=1}^{n}\left(\frac{\partial F_j}{\partial\Theta_\kappa}\cdot\frac{\partial F_\eta}{\partial\Theta_\kappa}\right);\ j=\overline{1,4}.
\end{aligned}\right\} \tag{14}$$

Для системи (4) $n=4$.

Розкладемо функції $m_2,\lambda_2,\lambda_3,k_2,k_3,k_4$ в ряди Тейлора в околі ϖ_i $\left(\varpi\in\{g,q,u,w\}\right)$.

Використовуючи вирази (12) — (14) для відповідних похідних та приводячи в (11) члени з однаковими степенями s^σ $\left(\sigma<\sigma_\varpi\right)$, отримаємо описані нижче співвідношення, що визначають шукані параметри розрахункових формул (5) — (10).

$$\left.\begin{aligned}
r_2 &= (\alpha_2,\xi_{21},\delta_{21},\gamma_{21},\beta_{21}),\\
r_3 &= (\alpha_3,\xi_{31},\delta_{31}+\delta_{32},\gamma_{31}+\gamma_{32},\beta_{31}+\beta_{32}),\\
r_3 &= (\alpha_4,\xi_{41},\delta_{41}+\delta_{42},\gamma_{41}+\gamma_{42}+\gamma_{43},\beta_{41}+\beta_{42}+\beta_{43}),
\end{aligned}\right\} \tag{15}$$

$$a_{11}=1; \tag{16}$$

$$e_{21}+e_{22}=1,\ 2e_{22}\cdot r_2=1; \tag{17}$$

$$\left.\begin{aligned}
s_{31}+s_{32}+s_{33}&=1,\\
\sum_{\kappa=2}^{3} s_{3\kappa}\cdot\prod_{i=1}^{\sigma-1} r_\kappa[j_i] &= \frac{1}{\sigma}\left(\sigma\in\{2,3\},j_1,j_2=\overline{1,5}\right),\\
s_{33}\cdot\gamma_{32}\cdot r_2&=\frac{1}{6}
\end{aligned}\right\} \tag{18}$$

$$s_{33}\cdot\delta_{32}\cdot r_2=\frac{1}{6};\ s_{33}\cdot\beta_{32}\cdot r_2=\frac{1}{6}, \tag{19}$$

$$D_1[b]\cdot\frac{\partial d}{\partial g}\approx 6s\cdot \tag{20}$$

З (18), (19) при $\alpha_2\notin\{0,2/3\},\alpha_3\neq 0,\alpha_2\neq\alpha_3$:

$$\left.\begin{aligned}
s_{31}&=\frac{6\alpha_2\alpha_3-3(\alpha_2+\alpha_3)+2}{6\alpha_2\alpha_3},\\
s_{32}&=\frac{3\alpha_3-2}{6\alpha_2(\alpha_3-\alpha_2)},\ s_{33}=\frac{2-3\alpha_2}{6\alpha_2(\alpha_3-\alpha_2)},\\
\xi_{21}&=\delta_{21}=\gamma_{21}=\beta_{21}=\alpha_2,\ \xi_{31}=\alpha_3,\\
\gamma_{31}&=\frac{\alpha_3[3\alpha_2(\alpha_2-1)+\alpha_3]}{\alpha_2(3\alpha_2-2)},\ \gamma_{32}=\frac{\alpha_3(\alpha_2-\alpha_3)}{\alpha_2(3\alpha_2-2)};
\end{aligned}\right\} \tag{21}$$

$$\delta_{31}=\frac{\alpha_3\left[\alpha_2\left(3\alpha_2-2\right)-\left(\alpha_2-\alpha_3\right)\right]}{\alpha_2\left(3\alpha_2-2\right)},\ \delta_{32}=\frac{\alpha_3\left(\alpha_2-\alpha_3\right)}{\alpha_2\left(3\alpha_2-2\right)};\tag{22}$$

$$\beta_{31}=\frac{\alpha_3\left[\alpha_2\left(3\alpha_2-2\right)-\left(\alpha_2-\alpha_3\right)\right]}{\alpha_2\left(3\alpha_2-2\right)},\ \beta_{32}=\frac{\alpha_3\left(\alpha_2-\alpha_3\right)}{\alpha_2\left(3\alpha_2-2\right)};\tag{23}$$

$$\left.\begin{gathered}\sum_{\kappa=1}^{4}p_{4\kappa}=1,\\ \sum_{\kappa=1}^{4}p_{4\kappa}\cdot\prod_{i=1}^{\sigma-1}r_\kappa\left[j_i\right]=\frac{1}{\sigma}\left(\sigma\in\{2,3,4\}\right),\\ p_{43}\cdot\beta_{32}\cdot r_3^\kappa\cdot\prod_{i=1}^{\sigma}r_2\left[j_i\right]+p_{44}\cdot r_4^\kappa\left(\beta_{42}\prod_{i=1}^{\sigma}r_\kappa\left[j_i\right]+\beta_{43}\prod_{i=1}^{\sigma}r_\kappa\left[j_i\right]\right)=R_{\sigma\kappa}\\ \left(\sigma=1\wedge\kappa<2\vee\sigma=2\wedge\kappa=0\right),\ R_{\sigma\kappa}=\frac{1}{2\sigma\left(3+\kappa\right)};\ j_1,j_2=1,5,\\ p_{44}\cdot\beta_{32}\cdot\beta_{43}\cdot r_2=1/24.\end{gathered}\right\}\tag{24}$$

Також, на підставі виразів (18), (19), можна записати наступні системи рівнянь.

$$\left.\begin{gathered}p_{43}\cdot\gamma_{32}\cdot r_3^\kappa\cdot\prod_{i=1}^{\sigma}r_2\left[j_i\right]+p_{44}\cdot r_4^\kappa\left(\gamma_{42}\prod_{i=1}^{\sigma}r_\kappa\left[j_i\right]+\gamma_{43}\prod_{i=1}^{\sigma}r_\kappa\left[j_i\right]\right)=R_{\sigma\kappa}\\ \left(\sigma=1\wedge\kappa<2\vee\sigma=2\wedge\kappa=0\right),\\ R_{\sigma\kappa}=\frac{1}{2\sigma\left(3+\kappa\right)};\ j_1,j_2=1,5,\\ p_{44}\cdot\gamma_{43}\cdot\gamma_{32}\cdot r_2=1/24,\\ p_{44}\cdot\beta_{43}\cdot\gamma_{32}\cdot r_2=1/24,\\ p_{44}\cdot\gamma_{43}\cdot\beta_{32}\cdot r_2=1/24;\end{gathered}\right\}\tag{25}$$

$$\left.\begin{gathered}\left(p_{43}\cdot\delta_{32}+p_{44}\cdot\delta_{42}\right)\cdot r_2=1/6,\\ \left(p_{43}\cdot\delta_{32}\cdot r_3+p_{44}\cdot\delta_{42}\cdot r_4\right)\cdot r_2\left[j\right]=1/8\ \left(j=\overline{1,5}\right),\\ \left(p_{43}\cdot\delta_{32}+p_{44}\cdot\delta_{42}\right)\cdot r_2\left[i\right]\cdot r_2\left[j\right]=1/12\ \left(i,j=\overline{1,5}\right),\\ p_{44}\cdot\beta_{43}\cdot\delta_{32}\cdot r_2=1/24,\\ p_{44}\cdot\gamma_{43}\cdot\delta_{32}\cdot r_2=1/24;\end{gathered}\right\}\tag{26}$$

$$\left.\begin{gathered}D_1\left[b\right]\cdot\frac{\partial h}{\partial g}\approx 6s^2,\\ D_1\left[b\right]\cdot D_1\left[\frac{\partial h}{\partial g}\right]\approx 8s^2,\\ D_2\left[b\right]\cdot\frac{\partial h}{\partial g}\approx 24s,\\ D_1\left[F_\kappa\right]\cdot\frac{\partial h}{\partial\Theta_j}\cdot\frac{\partial F_j}{\partial\Theta_\kappa}\approx 24s,\ \left(\kappa=1\wedge j<5\vee\kappa>1\wedge j<3\right).\end{gathered}\right\}\tag{27}$$

Щоб отримати співвідношення для загального випадку розрахункових параметрів виду (6) — (10), розглянемо систему

$$\frac{d\Theta}{dx} = F(x, \Theta), \tag{28}$$

в кожній групі якої по два рівняння:

$$\left.\begin{aligned} \mathbf{\Theta} &= (G, g, Q, q, U, u, W, w)^{\mathrm{T}}, \\ \mathbf{F} &= (a, b, c, d, e, f)^{\mathrm{T}}. \end{aligned}\right\} \tag{29}$$

Позначимо параметри для розрахункових приростів $\Delta\mathbf{\Psi}\ (\mathbf{\Psi} \in \{G, Q, U, W\})$ знову уведених змінних G, Q, U, W так, як у (6) із заміною у останніх рядкових літер заголовними.

Аналогічно (15) позначимо

$$\left.\begin{aligned} r_j = \left(\alpha_j, \mathrm{E}_{j1}, \xi_{j1}, \sum_{i=1}^{i_3} \Delta_{ji}, \sum_{i=1}^{i_4} \delta_{ji}, \sum_{i=1}^{i_5} \Gamma_{ji}, \sum_{i=1}^{i_6} \gamma_{ji}, \sum_{i=1}^{i_7} \mathrm{B}_{ji}, \sum_{i=1}^{i_8} \beta_{ji} \right) \\ (j = 2, 3, 4; \text{якщо } j = 4 \wedge 2 < \kappa < 5, \text{то } \mathrm{i}_\kappa = 2, \text{інакше } i_\kappa j - 1). \end{aligned}\right\} \tag{30}$$

Тоді можна записати:

$$N_1 = sa_i, n_1 = sb_1, \tag{31}$$

$$M_1 = s\sigma;$$

$$M_2 = s\sigma(x_i + \alpha_2 \cdot s, G_i + \mathrm{E}_{21} \cdot N_1, g_i + \xi_{21} \cdot n_1, Q_i + \Delta_{21} \cdot M_1, g_i + \delta_{21} \cdot m_1,$$

$$U_i + \Gamma_{21} \cdot \Lambda_i, u_i + \gamma_{21} \div \lambda_1 \cdot W_1 + \mathrm{B}_{21} \cdot K_1, w_i + \beta_{21} \cdot k_1) = s\sigma(x_i, \Theta_i, r_2); \tag{32}$$

$$m_1 = sc_1, m_2 = sc(x_i, \Theta_i, r_2); \tag{33}$$

$$\Lambda_i = s \cdot h_i, \Lambda_j = s \cdot h(x_j, \Theta_{i,}\ r_j)(j = 2, 3); \tag{34}$$

$$\lambda_i = s \cdot g_i, \lambda_j = s \cdot g(x_j, \Theta_{i,}\ r_j)(j = 2, 3); \tag{35}$$

$$K_i = s \cdot e_i, K_j = s \cdot e(x_j, \Theta_{i,}\ r_j)(j = 2, 3, 4); \tag{36}$$

$$k_i = s \cdot f_i, k_j = s \cdot f(x_j, \Theta_{i,}\ r_j)(j = 2, 3, 4); \tag{37}$$

Як і в (11), (12) маємо:

$$\Delta\varpi_i = \Delta\varpi + O(s^{\sigma\varpi}),$$

$$\varpi \in \{G, g, Q, q, U, u, W, w\}, \tag{38}$$

$$D_j[\varpi] = \left(\frac{\partial}{\partial x} + \sum_{j=1}^{n} F_j \cdot \frac{\partial}{\partial \Theta_j} \right)^{\sigma} [\varpi]. \tag{39}$$

Для системи (28) $n = 8$.

Повторюючи процедуру отримання співвідношень (16) — (27), можна переконатися у справедливості інтерпретації співвідношень (16) — (27) для системи (28), яка пояснюється нижче.

У подальших розмірковуваннях вагові коефіцієнти t_{ij}, s_{ij}, p_{ij} для параметрів (32), (34), (36) поміняємо на коефіцієнти T_{ij}, S_{ij}, P_{ij}, відповідно.

Для груп рівнянь, що відповідають компонентам F_j системи (28) та таких, що розв'язуються за умовою методом не нижче четвертого порядку, повинні виконуватися,

по-перше, співвідношення (24) — (26), а також будемо вимагати при цьому заміну в (25) величин ϖ на певне їх наближення $\widehat{\varpi}$. По друге, повинні виконуватися співвідношення (24) — (26) із заміною в них коефіцієнтів p_{ij} на P_{ij} (також в вимогою заміну в (25) величин ϖ на певне їх наближення $\widehat{\varpi}$). По-третє, спільний розв'язок методом четвертого порядку не одного, а двох рівнянь четвертої групи системи (28) призводить до необхідності виконання співвідношень

$$\left.\begin{gathered} P_{43}\cdot\beta_{32}\cdot r_3^{\kappa}\prod_{i=1}^{\sigma} r_2[j_i]+P_{44}\cdot r_4^{\kappa}\left(\beta_{42}\prod_{i=1}^{\sigma} r_2[j_i]+\beta_{42}\cdot\prod_{i=1}^{\sigma} r_3[j_i]\right)=\frac{1}{2\sigma(3+\kappa)} \\ (\sigma=1\wedge\kappa<2\vee\sigma=2\wedge\kappa=0,\ j_1,j_2<n+2), \\ P_{44}\cdot\beta_{32}\cdot\beta_{43}\cdot r_2=1/24, \\ P_{44}\cdot\beta_{32}\cdot B_{43}\cdot r_2=1/24, \\ P_{44}\cdot B_{32}\cdot\beta_{43}\cdot r_2=1/24, \end{gathered}\right\} \tag{40}$$

подібних залежностям (25). Наостанок, крім як описаним співвідношенням, розрахункові параметри (32) — (37) для системи (28) повинні задовольняти аналогічним (19), (22), (23), (26), (27) залежностям, які визначають узгодження розрахункових параметрів для груп рівнянь, які розглядається та входять (в свою чергу) до системи, що інтегрується:

$$\Delta_{32}\cdot r_2=\delta_{32}\cdot r_2=\Gamma_{32}\cdot r_2=\gamma_{32}\cdot r_2 B_{32}\cdot r_2=\beta_{32}\cdot r_2=\frac{1}{6S_{33}}\cdot \tag{41}$$

$$\left.\begin{gathered} \left(P_{43}\cdot\Delta_{32}\cdot r_3^{\kappa}+P_{44}\cdot\Delta_{42}\cdot r_4^{\kappa}\right)\cdot\prod_{i=}^{\sigma} r_2[j_i]=R_{\sigma\kappa}, \\ \left(P_{43}\cdot\Delta_{32}\cdot r_3^{\kappa}+P_{44}\cdot\delta_{42}\cdot r_4^{\kappa}\right)\cdot\prod_{i=}^{\sigma} r_2[j_i]=R_{\sigma\kappa}, \\ \varpi_{43}\cdot\Gamma_{32}\cdot\prod_{i=1}^{\sigma} r_2[j_i]+\varpi_{44}\left(\Gamma_{42}\cdot\prod_{i=}^{\sigma} r_2[j_i]+\Gamma_{43}\cdot\prod_{i=}^{\sigma} r_3[j_i]\right)=R_{\sigma\kappa}, \\ \varpi_{43}\cdot\gamma_{32}\cdot\prod_{i=1}^{\sigma} r_2[j_i]+\varpi_{44}\left(\gamma_{42}\cdot\prod_{i=}^{\sigma} r_2[j_i]+\gamma_{43}\cdot\prod_{i=}^{\sigma} r_3[j_i]\right)=R_{\sigma\kappa}, \\ \varpi_{43}\cdot B_{32}\cdot\prod_{i=1}^{\sigma} r_2[j_i]+\varpi_{44}\left(B_{42}\cdot\prod_{i=}^{\sigma} r_2[j_i]+B_{43}\cdot\prod_{i=}^{\sigma} r_3[j_i]\right)=R_{\sigma\kappa}, \\ \varpi_{43}\cdot\beta_{32}\cdot\prod_{i=1}^{\sigma} r_2[j_i]+\varpi_{44}\left(\beta_{42}\cdot\prod_{i=}^{\sigma} r_2[j_i]+\beta_{43}\cdot\prod_{i=}^{\sigma} r_3[j_i]\right)=R_{\sigma\kappa}, \\ \varpi_{43}=P_{43}\cdot r_3^{\kappa},\ \varpi_{44}=P_{44}\cdot r_4^{\kappa}, \\ R_{\sigma\kappa}=\frac{1}{2\sigma(3+\kappa)}, \\ (\sigma=1\wedge\kappa<2\vee\sigma=2\wedge\kappa=0,\ j_1,j_2<n+2), \end{gathered}\right\} \tag{42}$$

$$\left.\begin{aligned}
&\Gamma_{43}\cdot\Delta_{32}=\gamma_{43}\cdot\Delta_{32}=\mathrm{B}_{43}\cdot\Delta_{32}=\beta_{43}\cdot\Delta_{32}=\frac{1}{24\,P_{44}\cdot r_2[j]},\\
&\Gamma_{43}\cdot\delta_{32}=\gamma_{43}\cdot\delta_{32}=\mathrm{B}_{43}\cdot\delta_{32}=\beta_{43}\cdot\delta_{32}=\frac{1}{24\,P_{44}\cdot r_2[j]},\\
&\Gamma_{43}\cdot\Gamma_{42}=\gamma_{43}\cdot\Gamma_{32}=\mathrm{B}_{43}\cdot\Gamma_{32}=\beta_{43}\cdot\Gamma_{32}=\frac{1}{24\,P_{44}\cdot r_2[j]},\\
&\Gamma_{43}\cdot\gamma_{32}=\gamma_{43}\cdot\Delta_{32}=\mathrm{B}_{43}\cdot\gamma_{32}=\beta_{43}\cdot\gamma_{32}=\frac{1}{24\,P_{44}\cdot r_2[j]},\\
&\Gamma_{43}\cdot\mathrm{B}_{32}=\gamma_{43}\cdot\mathrm{B}_{32}=\mathrm{B}_{43}\cdot\mathrm{B}_{32}=\beta_{43}\cdot\mathrm{B}_{32}=\frac{1}{24\,P_{44}\cdot r_2[j]},\\
&\Gamma_{43}\cdot\beta_{32}=\gamma_{43}\cdot\beta_{32}=\mathrm{B}_{43}\cdot\beta_{32}=\beta_{43}\cdot\beta_{32}=\frac{1}{24\,P_{44}\cdot r_2[j]},\\
&\left(j=\overline{1,n+1}\right);
\end{aligned}\right\} \qquad (43)$$

$$\left.\begin{aligned}
&D_1[F_j]\cdot\frac{\partial F_\kappa}{\partial\Theta_j}\approx 6s\ \left(\kappa=5\wedge j=1\vee\kappa=6\wedge j=2\right),\\
&D_1[F_j]\cdot D_1\left[\frac{\partial F_\kappa}{\partial\Theta_j}\right]\approx 8s\ \left(\kappa>6\wedge j<3\right),\\
&D_1[F_j]\cdot\frac{\partial F_\kappa}{\partial\Theta_j}\approx 24s\ \left(j<3\wedge\kappa>6\right),\\
&D_1[F_j]\cdot\frac{\partial F_\kappa}{\partial\Theta_j}\cdot\frac{\partial F_j}{\partial\Theta_\kappa}\approx 24s\ ,\\
&\left(\kappa<3\wedge j=\overline{1,n}\vee\kappa>2\wedge j<5\right).
\end{aligned}\right\} \qquad (44)$$

З отриманих співвідношень видно, що вибір однакових параметрів $\bar{r}_j=r_j$, $\hat{r}_j=r_j$, $\tilde{r}_j=r_j$ для всіх рівнянь відповідної групи забезпечує можливість застосування розрахункових співвідношень (16) — (26) для системи з довільним числом рівнянь у кожній групі змінних.

Отримані співвідношення містять той окремий випадок, коли використовуються розрахункові формули, що забезпечують один порядок похибки на кроці інтегрування для всіх рівнянь системи. При цьому із співвідношень (8) — (17) отримуються розрахункові формули другого порядку, з (9) — (18) — третього порядку, а з (10) — (24) — четвертого порядку. Зазначимо, що ці співвідношення обмежують вектор вільних параметрів розрахункових формул наступним чином:

— Для порядку методу $\sigma=2$:

$$\alpha_2\neq 0\,,\ \delta_{21}=\alpha_2\,,\ e_{22}=\frac{1}{2\alpha_2}\,,\ e_{21}=1-e_{22}\,. \qquad (45)$$

— Для порядку методу $\sigma=3$:

$$\alpha_2\neq 0\ \text{б}\ \gamma_{32}\neq 0\,.$$

Розглянемо можливості, які є при цьому:

1. $\alpha_2=\alpha_3=2/3\,,\ \gamma_{31}=2/3-\gamma_{32}\,.$

Ця умова тягне за собою вибір

$$s_{33} = \frac{1}{4\gamma_{32}},\ s_{32} = 3/4 - s_{33},\ s_{31} = 1/4. \tag{46}$$

2. $\alpha_2 = 2/3,\ \alpha_3 = 0,\ \gamma_{31} = 2/3 - \gamma_{32},\ s_{33} = \dfrac{1}{4\gamma_{32}},\ s_{32} = 1/4,$

$$s_{31} = 1/4 - s_{33}. \tag{47}$$

3. Можливий також наступний випадок параметрів

$$\left.\begin{array}{c} \alpha_2 = 1,\ \alpha_3 \notin \{0, 2/3, 1\},\ \gamma_{31} = \alpha_3^2,\ \gamma_{32} = \alpha_3(1-\alpha_3), \\ s_{33} = \dfrac{1}{6\alpha_3(1-\alpha_3)},\ s_{32} = \dfrac{2-3\alpha_3}{6(1-\alpha_3)},\ s_{33} = \dfrac{3\alpha_3 - 1}{6\alpha_3}; \end{array}\right\} \tag{48}$$

4. $\alpha_3 = 1,\ \alpha_2 \notin \{0, 2/3, 1\}.$

5. $\alpha_2 \notin \{0, 2/3, 1\},\ \alpha_3 \notin \{0, 2/3, 1\},\ \alpha_2 \neq \alpha_3.$

При цьому параметри γ_{31}, γ_{32} та вагові коефіцієнти s_{31}, s_{32}, s_{33} обчислюються за формулами (21).

— Для порядку методу $\sigma = 4$ система (24) несумісна при

$$\alpha_2 = 0 \vee \alpha_3 = 1 \vee \alpha_3 \wedge \alpha_2 \neq 1/2 \vee \alpha_2 = 1/2 \wedge \alpha_3 \notin \{0, 1/2\}.$$

Залишаються наступні можливості:

1. $\alpha_2 = \alpha_3 = 1/2.$

Цей вибір дає параметри розрахункової формули четвертого порядку, які найбільш широке використовуються:

$$\left.\begin{array}{c} \beta_{21} = \beta_{32} = 1/2,\ \alpha_4 = 1,\ \beta_{31} = \beta_{41} = \beta_{42} = 0,\ \beta_{43} = 1, \\ p_{41} = p_{44} = 1/6,\ p_{42} = p_{43} = 1/3. \end{array}\right\} \tag{49}$$

2. $\alpha_2 = 1/2,\ \alpha_3 = 0,\ \beta_{32} \neq 0.$

Цей вибір дає такі параметри:

$$\left.\begin{array}{c} \beta_{31} = -\beta_{32},\ \beta_{41} = -[1/2(1 + 1/\beta_{32})],\ \beta_{42} = 3/2,\ \beta_{43} = 1/2\beta_{32}, \\ p_{41} = [1/6(1 - 1/2\beta_{32})],\ p_{42} = 2/3,\ p_{43} = 1/12\beta_{32},\ p_{44} = 1/6. \end{array}\right\} \tag{50^1}$$

3. $\alpha_2 = 1,\ \alpha_3 = 1/2,\ p_{44} \neq 0.$

Цей вибір дає такі параметри:

$$\left.\begin{array}{c} \beta_{31} = 3/8,\ \beta_{41} = 1/8,\ \beta_{41} = [1 - (1/4p_{44})],\ \beta_{42} = -1/12p_{44},\ \beta_{43} = -1/3p_{44}, \\ p_{41} = 1/6,\ p_{42} = 1/6 - p_{44},\ p_{43} = 1/3.. \end{array}\right\} \tag{50^2}$$

4. Можливий також наступний випадок параметрів

$$\left.\begin{gathered}
\alpha_2 \notin \{0,1/2,1\},\ \alpha_3 \notin \{0,1/2,1\},\ \alpha_2 \neq \alpha_3 .\\
p_{42} = 1/12\alpha_2 \cdot (1-2\alpha_3)/(\alpha_2-\alpha_3)\cdot 1/(1-\alpha_2),\cdot\\
p_{43} = 1/12\alpha_3 \cdot (12\alpha_2-1)/(\alpha_2-\alpha_3)\cdot 1/(1-\alpha_3),\cdot\\
p_{44} = 1/12 \cdot [3+6\alpha_2\alpha_3 - 4(\alpha_2+\alpha_3)/(1-\alpha_2)(1-2\alpha_3)],\\
\beta_{32} = [1/24(1-\alpha_3)\cdot\alpha_2\cdot p_{43}],\ \beta_{31} = \alpha_3 - \beta_{32},\\
\beta_{42} = \{[2-4(1-\alpha_3)\cdot\alpha_3 - (\alpha_2+\alpha_3)]/24(1-\alpha_3)\cdot(\alpha_2-\alpha_3)\cdot\alpha_2\cdot p_{44}\},\\
\beta_{43} = \{(2\alpha_2-1)/[12\alpha_3\cdot(\alpha_2-\alpha_3)\cdot p_{44}]\},\ \beta_{41} = 1-(\beta_{42}+\beta_{43}).
\end{gathered}\right\} \qquad (51)$$

Із використанням отриманих співвідношень для конкретної задачі (1) — (3), що досліджується, можна віднайти розбиття ММ на групи, які при моделюванні системи *мінімізують час розв'язування задачі Коші*, задовольняючи вимогам точності щодо розв'язку цієї задачі.

Необхідно зазначити дві обставини. Отримані співвідношення (16) — (43) для розрахункових формул (31) — (37) різник порядків, що застосовуються до відповідних груп рівнянь ММ досліджуваної системи (1) — (3), є вірними при нехтуванні у (38) величинами $O\left(s^{\sigma\varpi}\right)$ і, крім того, за умов (20), (27), (44).

Також, для будь-яких поєднань порядків розрахункових формул (31) — (37), що застосовуються, можна задовольняти співвідношенням (16) — (43), крім поєднання формул 3-го порядку, що застосовуються до однієї групи рівнянь, і 4-го порядку, що застосовуються до іншої групи рівнянь. У цьому випадку залишається невиконаним хоча б одне із співвідношень (18) — (26).

Наприклад, вибір (49) параметрів розрахункової формули 4-го порядку разом з параметрами

$$\left.\begin{gathered}
\alpha_2 = 1/3,\ \alpha_3 = 1/2,\ \beta_{32} = 1/4,\ \gamma_{32} = 3/8,\\
\gamma_{32} = 3/4,\ \gamma_{42} = 3/2,\ \gamma_{43} = 2.
\end{gathered}\right\} \qquad (52)$$

задовольняє усім співвідношенням (17) — (25), крім

$$s_{33}\cdot\beta_{32}\cdot\alpha_2 = C_{\text{к}}. \qquad (53)$$

Обрані параметри дають значення $C_{\text{к}} = 1/4$ замість потрібного $C_{\text{к}} = 1/6$. Зазначимо, що $C_{\text{к}} \to 1/6$ при $\alpha_2 \to 0$, але при цьому зростають ваги s_{31} та s_{32}, і зменшення цієї компоненти методичної похибки може призвести до збільшення обчислювальних похибок визначення шуканих прирощень $\Delta\varpi$.

Зробивши замість (52) наступний вибір параметрів:

$$\left.\begin{gathered}
\alpha_2 = 1/16,\ \alpha_3 = 3/4,\ \beta_{31} = 9/56,\ \beta_{32} = 33/56,\\
\gamma_{31} = -153/58,\ \gamma_{32} = 33/7,\\
\delta_{21} = 1/2,\ \gamma_{31} = -7/2,\ \gamma_{32} = 4,\ \gamma_{41} = 7/3,\ \gamma_{42} = -24/11,\ \gamma_{43} = 28/33,\\
s_{31} = -5/9,\ s_{32} = 32/33,\ s_{33} = 58/99,
\end{gathered}\right\} \qquad (54)$$

отримуємо у (53) значення $C_{\text{к}} = 29/28\cdot 1/6$, що є близьким до необхідного $C_{\text{к}} = 1/6$.

Наведені співвідношення (16) — (43) дають можливість для конкретної задачі моделювання нестаціонарної системи, заданою ММ виду (1) — (3), та оцінки точності характеристик цієї досліджуваної системи побудувати блок програм, що реалізує пошук значень параметрів розрахункових формул (31) — (37), які мінімізують часові витрати при допустимій точності оцінок необхідних характеристик. Долучення цього блоку у комплект програм забезпечення імітаційного моделювання, дає можливість оцінки необхідних характеристик якості досліджуваних нестаціонарних (динамічних)

систем достатньо загального виду з придатними точністю та швидкодією системи моделювання (тобто системи, що реалізує ММ виду (1) — (3)).

Висновок. Визначено, що при реалізації ММ нестаціонарних систем в задачах моделювання, управління та ідентифікації ефективним числовим методом є методо Рунге-Кутти, який забезпечує отримання необхідної точності розв'язку задачі. При цьому зазначено, що на досягнення бажаної точності розв'язку значно впливає крок інтегрування, який, в свою чергу, визначається динамічними властивостями досліджуваної системи. За наявності в ММ нестаціонарної системи параметрів, що суттєво відмінним чином характеризують її динаміку, ускладнюється процедура вибору кроку інтегрування в методі Рунге-Кутти, який би забезпечував необхідну точність отриманого розв'язку.

Показано, що дієвим шляхом при отриманні бажаної точності розв'язку, є розбиття вихідної задачі для попередньо виділених груп координат (параметрів) з різними швидкостями зміни та відмінними залежностями координат від аргументу в ММ нестаціонарної системи. Це дає змогу варіювання при виборі кроку інтегрування та порядку методу Рунге-Кутти для кожної з виділених груп параметрів.

Отримано розрахункові вирази щодо обчислення необхідних порядків числового методу при розбитті на групи параметрів, які (порядки) зумовлюють аналітичне визначення кроку інтегрування та забезпечують необхідну точність шуканого розв'язку.

На тестовому прикладі показано застосування отриманих розрахункових формул і можливість проведення аналізу щодо ефективності останніх при виборі порядку методу та забезпеченні бажаної точності розв'язку задачі реалізації ММ нестаціонарної системи.

Список літератури

1. Chan R., Tsai A. On explicit two-derivative Runge – Kutta methods. *Numerical Algorithms*. 2010. Vol. 53. P. 171-194.
2. Okten Turaci M., Ozis T. Derivation of three-derivative Runge – Kutta methods. *Numerical Algorithms*. 2017. Vol. 74(1). P. 247-265.
3. Iserles A., Norsett S.P. On the theory of parallel Runge-Kutta methods. *IMA J. Numer. Anal.* 2009. Vol. 10. P.463-488.
4. Owren B., Zennaro M. Derivation of efficient continuous explicit Runge – Kutta methods. *SIAM J. Sci. and Stat. Comput.* 2016. Vol. 13. No. 6. P. 1488–1501.
5. Hairer E. Order conditions for numerical methods for partitioned ordinary differential equations. *Numer. Math.* 2011. Vol. 36. P. 431–445.
6. Dormand, J. R., El-Mikkawy M.E.A., Prince P. J. Families of Runge – Kutta Formulas. *IMA J. Numer. Anal.* 2007. Vol. 7. P. 235–250.

PARAMETERS OF THE RUNGE-KUTTA METHOD WITH DIFFERENT ORDER OF ACCURACY IN THE INTEGRATION OF DYNAMICS EQUATIONS IN THE PROBLEMS OF MODELLING NON-STATIONARY SYSTEMS

S. A. Polozhaenko, A. Yu. Prokofiev

National Odesa Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine
emails: sanp277@gmail.com, fallbrick@gmail.com

In the creation and research of modeling, control and identification systems, the most important stages are the formulation and numerical solution of equations of mathematical models of these systems, which are usually represented in the classes of differential and integral equations. At the same time, the issues of developing and researching computational algorithms that implement methods for numerical solution of equations of mathematical models of systems, in particular, ensuring control over the accuracy of the desired solution, as well as assessing the impact of deviations of parameters of dynamic systems on their movement and quality indicators, are crucial.

Both in analyzing the accuracy of numerical study of mathematical models of dynamic systems and in solving problems of synthesis of the latter based on accuracy conditions, the possibility of analytical expression of additional motion of the excited system is of great importance.

Mathematical models of non-stationary systems, represented in the form of differential equations in full derivatives, are implemented in the vast majority of applied problems by the Runge-Kutta method of various orders. It is shown that an increase in the productivity of machine calculation can be achieved if it is possible to take into account the difference in the rate of change of different groups of coordinates of the investigated non-stationary system. The problem is formulated and the possibility of rational choice of parameters of the Runge-Kutta method formulas is considered, which allows minimizing the time of integration of equations of the mathematical model of the system.

Keywords*:* unsteady system, mathematical model, numerical method, Runge-Kutta method, method order, solution accuracy.

DOI 10.15276/imms.v14.no1-2.97
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 97-107

РОЗРОБКА ПРОГРАМНОГО ЗАСТОСУНКУ ДЛЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА СТИЛЕМ НАБОРУ НА КЛАВІАТУРІ

Д. М. Слабенко[1], О.А. Стопакевич[1], А. О. Стопакевич[2]

[1] Національний університет «Одеська політехніка»,
1, Шевченка пр., м.Одеса, 65044, Україна
email: stopakevich@op.edu.ua
[2] Державний університет інтелектуальних технологій та зв'язку,
1, Кузнечна вул., м.Одеса, 65029, Україна
email: stopakevich@gmail.com

В статті розглядається розробка програмного забезпечення для біометричної ідентифікації користувачів за стилем набору на клавіатурі. Біометрична автентифікація, зокрема, методи, що базуються на поведінкових характеристиках, набувають все більшої популярності завдяки своїй здатності забезпечувати безпеку без необхідності запам'ятовування паролів. Розробка системи біометричної ідентифікації на основі набору тексту, введеного користувачем на клавіатурі, є привабливим рішенням, оскільки не лише потенційно забезпечує доволі надійну ідентифікацію, а й не потребує витрат на спеціальне обладнання. В роботі наведено перелік факторів, які впливають на процес набору тексту, таких як час натискання клавіш, швидкість друку, частота помилок та інші, які можуть варіюватися в залежності від індивідуальних особливостей користувача. Також обговорюються недоліки біометричної ідентифікації, зокрема, вплив зовнішніх факторів, таких як втома або відволікання, на точність аутентифікації. На основі аналізу параметрів, відомих методів та підходів до біометричної ідентифікації за стилем набору на клавіатурі запропоновано новий алгоритм перевірки, який базується на аналізі інтервалів часу натискання та пошуку клавіш, що дозволяє визначити відповідність між збереженим профілем користувача та його поточним набором тексту. Для зменшення впливу зовнішніх факторів рекомендується використовувати фіксований текст обсягом не менше 300 символів. Результати експериментів, проведених за допомогою розробленого програмного застосунку, підтверджують ефективність розробленого програмного забезпечення на основні запропонованого алгоритму ідентифікації. Результати демонструють достатню надійність та точність у процесі ідентифікації. Робота має практичне значення для розробки нових методів безпеки в інформаційних технологіях, шляхом впровадження біометричних систем у різних сферах.

Ключові слова*:* біометрія, поведінкова, ідентифікація, авторизація, клавіатура, набір, користувач, програмне, забезпечення, профіль, метод, алгоритм

Вступ. Розвиток технологій призводить до того, що все більше конфіденційної інформації, поширення якої є небажаним, зберігається на цифрових пристроях. Отже, актуальною стає проблема розробка безпечних та економічно ефективних механізмів автентифікації.

Одним з підходів, який розвивається останнім часом, є біометрична ідентифікація особи. Крім класичних відбитків пальців, розвиваються технології ідентифікації за фотографією, голосом тощо. Недоліком цих методів є необхідність в застосуванні окремих приладів, складність діагностики. Тобто якщо ідентифікація не проходить, то доволі складно зрозуміти причину й провести додаткові дослідження причин цього. Методи ідентифікації за мовою, письмом, ходьбою, рухом та набором на клавіатурі відомі, як поведінкова біометрія. Перевагою цих методів над фізіологічним аналогом є здатність працювати в прихованому режимі. Недоліком є мінливість характеристик в залежності від стану здоров'я, фізичних пошкоджень тощо, що впливає на точність ідентифікації. Ще одним методом біометричної ідентифікації є біометрія натискання

клавіш. Вона пов’язана з вимірюванням та оцінкою ритму друку людини на цифрових пристроях. Під таким пристроєм зазвичай мається на увазі комп'ютерна клавіатура, мобільний телефон або сенсорна панель. Форма цифрового сліду створюється при взаємодії людини з цими пристроями. Вважається, що ці сигнатури багаті когнітивними якостями, які достатньо унікальні для кожної людини й мають великий потенціал для ідентифікації користувача [1]. Застосування біометричної ідентифікації за набором на клавіатурі дозволяє реалізувати процедуру ідентифікації як одночасно достатньо надійну, так й таку яка не вимагає додаткових економічних витрат на придбання обладнання для біометричної ідентифікації.

Задачею статті є розробка та дослідження програмного застосунку для біометричної ідентифікації за набором на клавіатурі, який базується на запропонованій метриці оцінки подібності набору з еталонним набором користувача.

Особливості біометричної ідентифікації за набором. Біометрична ідентифікація за набором має принципові особливості, якими не можна зневажати. Вона поступається з точки зору точності аутентифікації через зміни в ритмі набору тексту, які можуть бути викликані такими зовнішніми факторами, як травма, втома або відволікання [2]. Характер набору тексту людиною може поступово змінюватися відповідно до звикання, розвитку навичок набору тексту, адаптації до пристроїв введення та інших факторів навколишнього середовища. Тому рекомендується постійно оновлювати збережений профіль натискання клавіш для порівняння [3, 4].

Параметри біометрії натискання клавіш. Серед факторів, які впливають на біометричну ідентифікацію користувача при наборі тексту на клавіатурі, можна виділити наступні [5]:

– час пошуку, тобто час, потрібний для знаходження кожної клавіши до її натискання;
– час натискання, тобто час утримання клавіши перед відпусканням [6, 7];
– час польоту, тобто час, коли натискається наступна клавіша;
– швидкість друку;
– час перерв / пауз при наборі тексту;
– кількість допущених помилок і врахування найпоширеніших помилок;
– техніка виправлення помилок користувачем при наборі тексту;
– тип локальної клавіатури, яка використовується (механічна та плівковій, мала та велика, пряма та вигнута клавіатури);
– набір проводиться правшею чи лівшою (аналіз частини клавіатури, яка ефективніше використовується);
– місце розташування клавіатури (на столі, на ногах, …);
– типову послідовності букв, яка найчастіше вживана в рідній мові користувача.

Аналіз літератури показує, що перші з перелічених параметрів є основними, а інші можуть бути використані для аналізу, як допоміжні.

Відмітимо, що ідентифікація користувача при біометричній ідентифікації може бути проведена тільки за набором тексту з достатньо великою кількістю символів. Згідно з дослідженням [8, 9], кількість символів має бути не меншою за 300, а в якості основних показників, які треба застосувати при ідентифікації, рекомендовано використати час польоту та час утримання, що видно з рис.1.

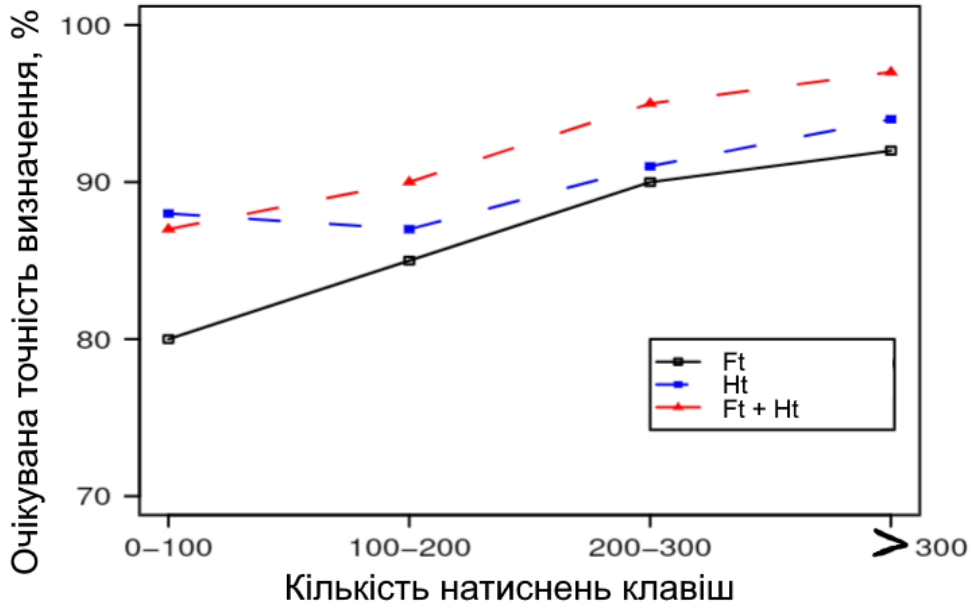


Рис. 1. Ефективність застосування основних параметрів: Ft – час польоту, Ht – час натиснення [8]

Запропонований алгоритм оцінки співпадіння набору еталонному профілю користувача. Звичайно алгоритми біометричної ідентифікації намагаються визначити подібність незалежно від тексту, який має набиратись. При наборі довільного тексту задача ідентифікації дуже складна. Орієнтація на диграми має свою раціональну мотивацію – людина набирає одне й теж слово в прямому й зворотному напрямку з різною швидкістю. Однак вона не враховує, що когнітивною одиницею набору тексту є слово, яке переводиться в натиснення окремих клавіш. Для людини характерна різна швидкість набору різних слів, яка обумовлена тим, наскільки часто таке слово набиралося людиною (прості слова, артиклі будуть набиратись швидше), наскільки людина грамотна і чи є мова набору її рідною мовою (треба замислюватись, як вірно набрати слово, чи ні), чи було визначено закінчення, чи викликає слово чи текст певні асоціації та думки. В такій мові, як англійська, є типові артиклі, закінчення, неправильні дієслова. Наприклад, зазвичай час набору артиклів “the”, “a”, прийменників “at”, “in”, закінчень “ing”, “ed”, дієслів типу “flet”, “was”, “been” тощо менший за час набору менш часто вживаних слів. Диграми частіше виділяються в наборі людину, яка застосовує сліпий десятипальцевий метод набору. Однак сліпий набор чітко виділяє й час натиснення окремих клавіш, оскільки в такому наборі є фіксоване положення пальців за замовченням, тому перехід з однієї клавіши на іншу обумовлений в першу чергу геометричною відстанню. Для людини, яка набирає просто кожний символ окремо й не тримає чіткої позиції рук, характеристики натиснення клавіш істотно залежать від слова.

Для зменшення впливу сторонніх факторів, біометричну автентифікацію ми пропонуємо визначати, використовуючи фіксований текст розміром понад 300 символів без регістру та розділювачів, й взяти за основу розкид параметрів користувача за кожною окремою клавішею.

Алгоритм перевірки вибраний наступний.

1. При формуванні профілю користувача – запам’ятати час пошуку та час натискання кожної літери тексту при наборі фіксованого тексту, що вводиться.
2. При ідентифікації – запропонувати ідентифікованої особі ввести той же текст і запам’ятати його.

Організувати цикл по всім літерам набраного тексту:

Якщо поточна літера по часу пошуку входить в діапазон часу еталонного набору

для даної літери

То додати таку літеру в тексті до лічильника g_1;

Інакше додати таку літеру в тексті до лічильника b_1;

Якщо поточна літера по часу натискання входить в діапазон часу еталонного набору для даної літери

То додати таку літеру в тексті до лічильника g_2;

Інакше додати таку літеру в тексті до лічильника b_2.

Критерієм проходження ідентифікації є умова $\left\{ \frac{b_1}{g_1} < 0.15 \ \& \ \frac{b_2}{g_2} < 0.15 \right\}$.

Програмна реалізація застосунку. Застосунок має включати дві програми, які реалізуємо мовою програмування Python для ОС Windows.

Перша програма реалізується з консольним інтерфейсом та аргументами командного рядка й має реалізовувати введення текстової фрази нижнім регістром без розділювальних знаків (про що користувача попереджують) та запис результатів цього введення в спеціальний JSON файл. При цьому застосовані такі бібліотеки для мови Python: sys, os, datetime, time, re, curses (windows), keyboard, beepy, json. Вибір введення натиснення клавіш саме в консольному застосунку обумовлено тим, що архітектура графічного інтерфейсу мови Python та взагалі ряду мов, які побудовані на концепції віртуальної машини, може призводити до значних похибок при отриманні часу натиснення клавіш в межах програмного інтерфейсу. Бібліотеки графічного інтерфейсу не націлені на отримання такого виду інформації, події звичайно орієнтуються на сам факт натиснення чи відтиснення клавіши. Нажаль, при введенні українською мовою в консолі виникають певні проблеми. Windows використовує розкладку cp866 для введення й в цій розкладці відсутня українська літера «і». Замість цього передбачається, що буква буде введена латинкою. Зміна кодування на cp1251 й Unicode призводить до інших проблем. В результаті, проблема біометрії клавіш латинкою розв'язується більш легко, а з українськими літерами виникають проблеми з бібліотеками curses та keyboard. З такої проблеми знайдено вихід в межах обмежень програмних бібліотек Python та програмного інтерфейсу Windows– вводити за фактом латинські літери, ігноруючи їх регістр, але відображати українські в консолі. Інтерфейс curses дозволяє відображати текст, що має бути набраний, й жовтим показує ту частину, яка вже набрана. В разі помилки подається за допомогою бібліотеки beep звуковий сигнал. Обробку кодів клавіш, подій натиснення та відтиснення реалізує бібліотека keyboard, ключовий метод – read_event(). Вимірювання часу між подіями клавіатури проводиться за допомогою time.perf_counter().

Залежно від аргументів командного рядка (sys) програма формує JSON файл з протоколом натискання як новий профіль, чи як результат перевірки відповідності певному профілю.

Підсистема працює у консолі за алгоритмом, показаним на рис. 2.

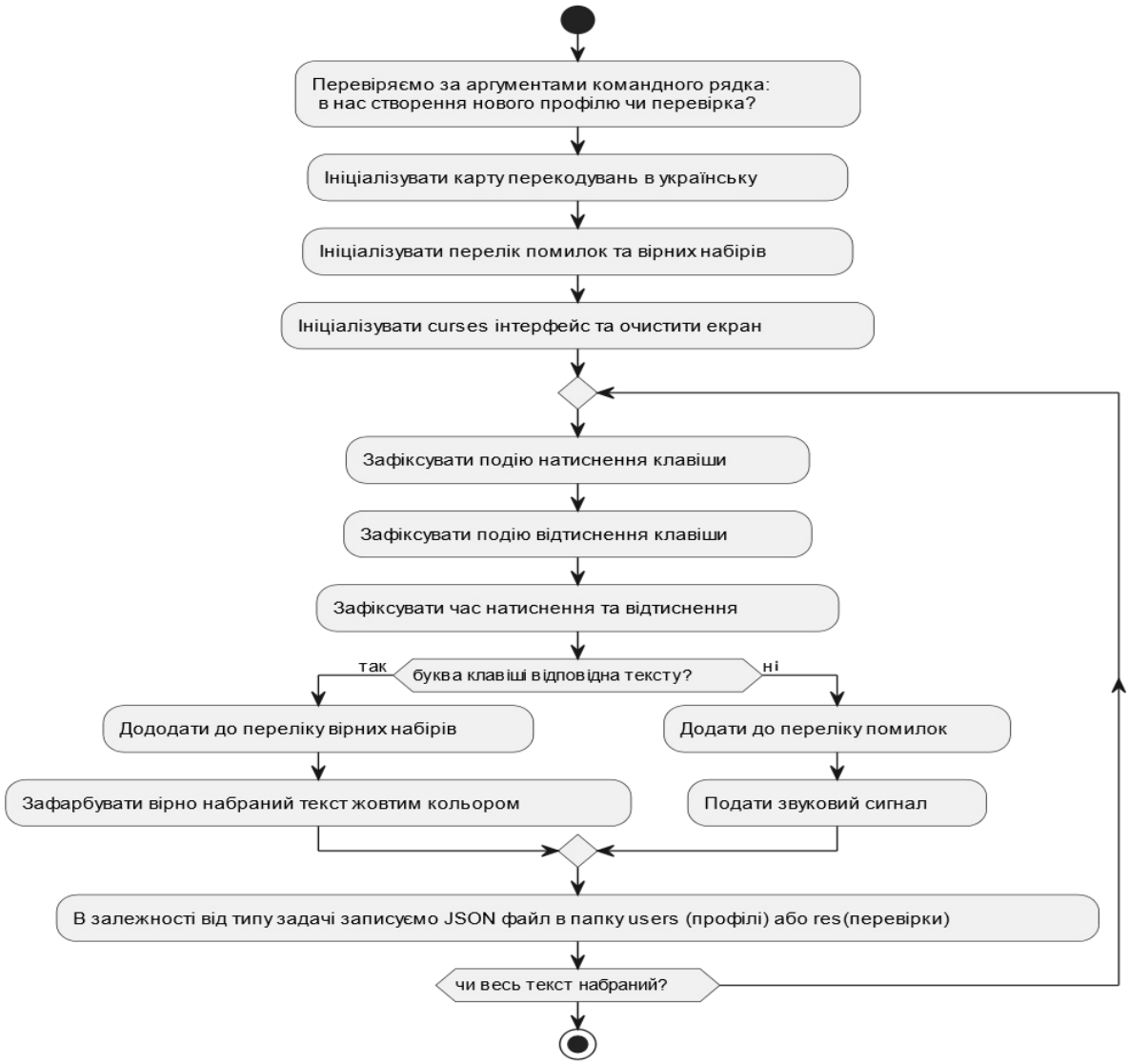


Рис. 2. Алгоритм роботи підсистеми для ідентифікації користувача

Підсистема приймає два аргументи командного рядка. Перший аргумент: new (новий профіль) чи check (перевірити профіль). Другий аргумент – ім'я користувача, яке має відповідати регулярному виразу

Зовнішній вигляд консольної програми, викликаної як python get_input.py new user3 в процесі набору тексту, показаний на рис. 3, 4.

```
d:\Program Files\python_keyboard_biometrics>python get_input.py new user3
Система підготовлена. Встановіть англійську розкладку якщо не стоїть.
Підготовтесь до набору та натисніть <enter>.
Набирайте зразу кібербезпека і далі.
```

Рис. 3. Попереджувальний текст – підготовка до набора фрази

```
Администратор: C:\Windows\System32\cmd.exe - python  get_input.py new user3
Кібербезпека це захищеність життєво важливих інтересів людини і громадянина суспільства та держави
під час використання кіберпростору за якої забезпечуються сталий розвиток інформаційного суспільства та
цифрового комунікативного середовища своєчасне виявлення запобігання і нейтралізація реальних і
потенційних загроз національній безпеці України у кіберпросторі.
```

Рис. 4. Процес набору фрази (жовтим відображена набрана частина)

Результативний JSON файл профілю user3 має наступний вигляд

{"text":
"\u041a\u0456\u0431\u0435\u0440\u0431\u0435\u0437\u043f\u0435\u043a\u0430
\u0446\u0435 …. ", "dt": "2024_05_03_19_19_14", "good": {"1": [0.4580399999395013,
0.08465239987708628, 19, "\u043a"], "2": [0.2832812999840826, 0.08598900004290044, 31,

"\u0456"], **….** "362": [0.20009749988093972, 0.08343700016848743, 31, "\u0456"], "363": [0.4003336001187563, 0.15026960009709, 53, "."]}, "fail": {"6": "\u0435", "27": "", "131": "\u0440", "150": "\u0441 \u0443", "154": "\u0441", "300": "\u043a \u043e", "360": "\u0440"}}

Друга програма має реалізовувати графічний інтерфейс для користувача. Цей інтерфейс має передбачати введення бази еталонних наборів користувачів (профілів), а також перевірку відповідності конкретного набору профілю заданого користувача.

Додаткова статистика може бути викликана при натисненні спеціальної клавіші. Ця статистика являє собою звіт у форматі веб сторінки (HTML), який містить детальну інформацію про набір користувача. Цей звіт може бути використаний як для аналізу причин того, чому процедура біометричної ідентифікації не вдалась, так і для подальшого удосконалення алгоритму ідентифікації. Крім інформації, що перевіряється, звіт містить також певну додаткову інформацію, яка використовується для ідентифікації інших параметрів біометричного набору, перелічених вище.

Для реалізації програми потрібні наступні програмні бібліотеки: tkinter, os, re, json, subprocess, ctypes, webbrowser, statistics.

Дослідження роботи застосунку у цілому. План досліджень наступний.

1. При створенні профілю Користувач №1 пише тестову фразу і вона буде збережена як профіль User1 (рис.5). Паралельно набір Користувача №1 запишемо програмою Keyboard Recorder.
2. При створенні профілю Користувач №2 пише тестову фразу й вона буде збережена як профіль User2 (рис.6).
3. Записаний набір Користувача №1 перевіримо на відповідність профілю User1.
4. Записаний набір Користувача №1 перевіримо на відповідність профілю User2.
5. Для перевірки сталості роботи програми Користувач №1 ще раз, через кілька днів, ідентифікується, написавши тестову фразу знов, й вона буде перевірена відносно профілю User1.

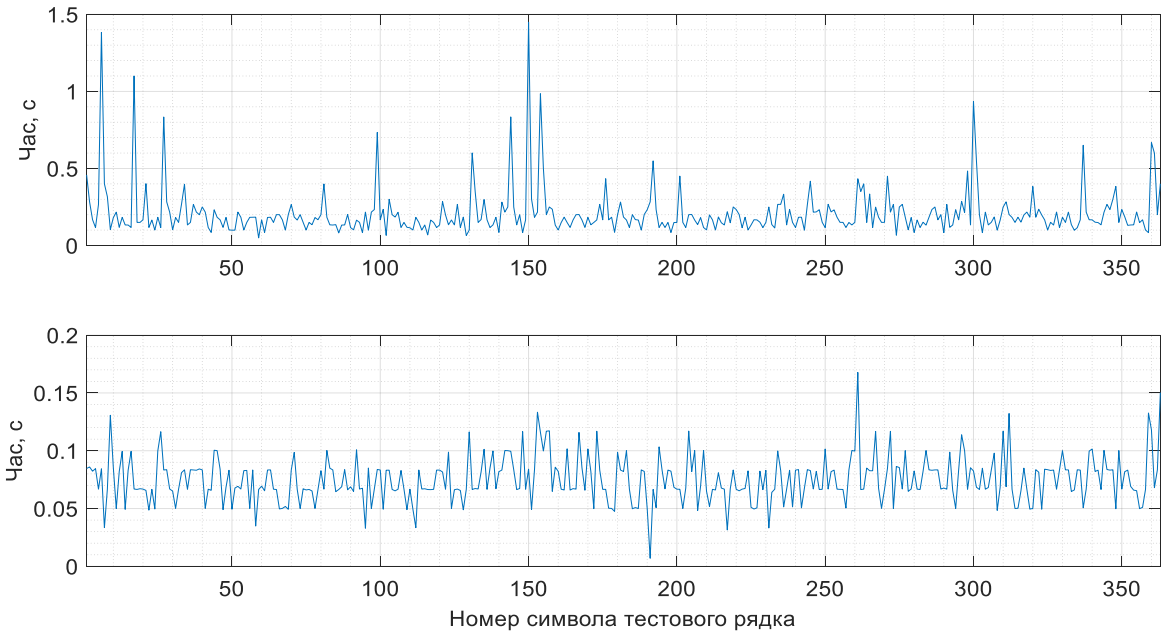


Рис. 5. Профіль користувача User1 (час пошуку та натискання)

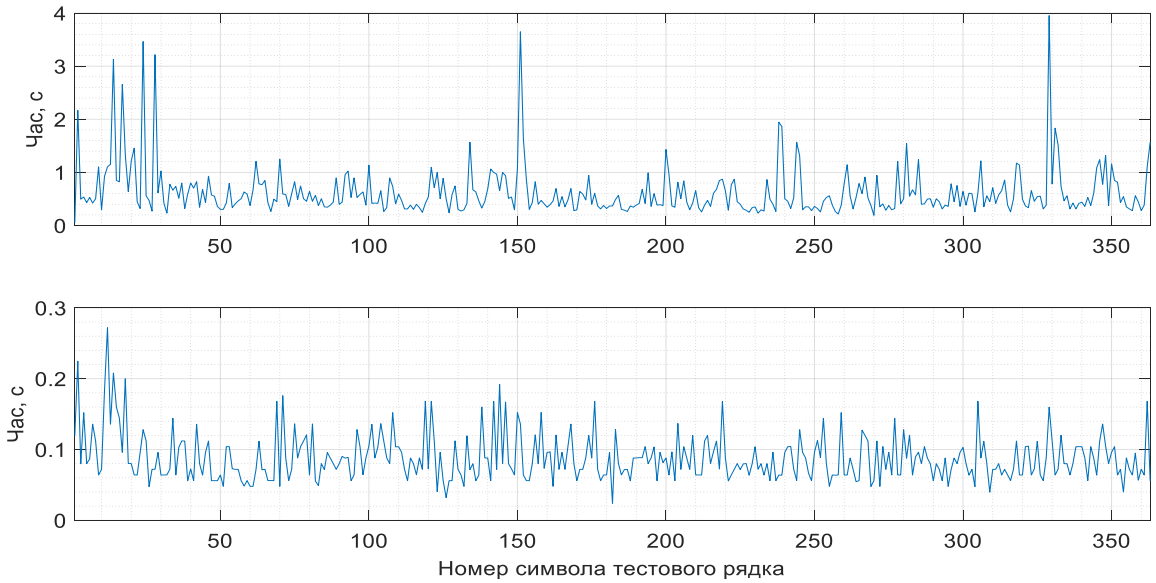


Рис. 6. Профіль користувача User2

Перевірка запису Keyboard Recorder за профілем користувача User1 показало майже повну відповідність за двома критеріями перевірки.

Перевірка запису Keyboard Recorder з профілем користувача User2 показало майже повну невідповідність за двома критеріями перевірки. За часом пошуку в інтервал потрапило лише 13 символів з 360, час часом натискання – 256 символів і 107 не попали. Таким чином, чітко бачимо, що це набирав інший користувач, ніж користувач User2.

Таким чином користувач був ідентифікований. Відсоток не співпадінь становив 8% для пошуку й 12% для натискання, що в цілому є допустимим відхиленням.

Проаналізуємо основні та додаткові параметри одного користувача, які можна отримати в програмі за допомогою звіту.

Закладений в критерії програми час натискання та інтервал його зміни дуже значимо залежить від літери. Це ми бачимо за фрагментом звіту, показаного на рис. 7. Наприклад, для букви «й» мінімальний час натискання – 0.09, а для «е» – 0.03. При чому різниця для букви «й» між мінімумом та максимумом не значна, а для буки «е» складає близько трьох раз.

Літера	Мінімум	Середнє	Максимум
	0.06625129998428747	0.08546933500256274	0.11693970000487752
а	0.0499716000049375	0.07146240356814815	0.10023859998909757
б	0.0833188000251539	0.08583101429394446	0.10027019999688491
в	0.049667099985526875	0.07210820666320311	0.0999491999973543
г	0.04892969998763874	0.06372225000814069	0.11619270002120174
д	0.06681400001980364	0.08627914000535383	0.09983479999937117
е	0.03331880000769161	0.06657056190167732	0.08352289997856133
ж	0.03340759998536669	0.06119966666058948	0.0834364999900572
з	0.06644220001180656	0.09562904545137743	0.16661909999675117
и	0.0499775999924168	0.0682624526272871	0.083427000005031
й	0.09987679999903776	0.10000601999927312	0.10007049998966977
к	0.05002150000655092	0.07000078999553808	0.08367729999008588
л	0.04999189998488873	0.07969094444221507	0.10020119999535382

Рис.7. Фрагмент звіту з мінімальним, середнім та максимальним значенням часу натискання літери при наборі тексту користувачем №1

Закладений в критерії програми час пошуку та інтервал його зміни теж дуже значимо залежить від літери. Це ми бачимо за фрагментом звіту, показаного на рис. 8. Наприклад, для букви «ж» мінімальний час пошуку – 0.2, а для «а» – 0.06. При чому, які й з часом натискання, різниця для букви «й» між мінімумом та максимумом не значна, а для літери «е» близько п’яти раз. Різниця для букви «з» більша за 10 раз. Між часом набору та часом пошуку присутня кореляція, однак вона має узагальнений характер. Наприклад найменший мінімальний час пошуку має літера «д», найбільший мінімальний час пошуку – літера «ж». Проте найменший мінімальний час натискання має літера «е», а найбільший мінімальний час натискання – літера «й».

Літера	Мінімум	Середнє	Максимум
	0.06661710000480525	0.17842948249672191	0.7331793999765068
а	0.06852640002034605	0.1918333607162432	0.8340992000012193
б	0.13348479999694973	0.3716093571399272	1.3676700000069104
в	0.08337020000908524	0.18473089333662454	0.40020110001205467
г	0.15020519998506643	0.1888071833285115	0.25035219997516833
д	0.06625430000713095	0.19037059999536723	0.2688532999891322
е	0.08349099999759346	0.15745305238219554	0.40035700000589713
ж	0.2001550999993924	0.21123473334591836	0.21681830001762137
з	0.09970639998209663	0.3137950181791728	1.1002237999928184
и	0.08341690001543611	0.15978699474362656	0.23417880001943558
й	0.15003119999892078	0.17343606000067666	0.18357929997728206
к	0.11687870000605471	0.22079115000087768	0.4589095000119414
л	0.11668909998843446	0.16308754444212858	0.2502237999869976

Рис.8. Фрагмент звіту з мінімальним, середнім та максимальним значенням часу пошуку літери при наборі тексту користувачем №1

На рис. 9 показані додаткові статистичні результати набору тексту користувачем №1.

Параметр	1 рядок	2 рядок	3 рядок	ліва частина	права частина
Мінімальний час пошуку	0.083	0.066	0.067	0.067	0.066
Середній час пошуку	0.207	0.208	0.211	0.203	0.229
Максимальний час пошуку	1.100	0.934	1.451	1.451	1.368
Мінімальний час натискання	0.033	0.033	0.007	0.007	0.033
Середній час натискання	0.073	0.071	0.081	0.072	0.077
Максимальний час натискання	0.167	0.133	0.150	0.133	0.167

а) перше тестування користувача №1

Параметр	1 рядок	2 рядок	3 рядок	ліва частина	права частина
Мінімальний час пошуку	0.088	0.080	0.080	0.080	0.088
Середній час пошуку	0.239	0.225	0.228	0.219	0.252
Максимальний час пошуку	1.584	1.504	1.200	1.584	1.504
Мінімальний час натискання	0.048	0.056	0.056	0.048	0.048
Середній час натискання	0.079	0.083	0.090	0.081	0.088
Максимальний час натискання	0.136	0.176	0.152	0.136	0.176

б) тестування користувача №1 через 5 днів

Рис. 9. Узагальнена статистика користувача №1 за рядками та частинами клавіатури

До додаткових результатів включено аналіз впливу такого фактору, як залежність параметрів набору від розташування клавіши у відповідному рядку клавіатури, її лівій та правій частині. З аналізу рис. 9 бачимо, що додаткові статистичні показники не дуже відтворились. Користувач – правша і користується десятипальцевим методом. Оскільки користувач правша, то, згідно з цим, показники мали б бути меншими на правій частині клавіатури. Тим не менш, бачимо, що виявлені показники таке правило порушують, більш стійкими до змін є максимальні показники. Мінімальний час пошуку в першому випадку дуже трохи менший на правій стороні, в другому випадку – навпаки. Середній час пошуку менший в лівій частині в обох випадках. Максимальний час пошуку трохи менше в правій частині в обох випадках. Мінімальний час натискання в першому випадку дуже відрізняються й менший в лівій стороні, в другому випадку – він однаковий. Середній час натискання в обох випадках трохи менше в лівій стороні. Максимальний час натискання у двох випадках менший в лівій стороні клавіатури. Таким чином, фактор «правша-лівша» не є значимим для використання при ідентифікації.

На рис. 10 досліджена залежність між кількістю символів в слові та часом набору слова (сума часу натиснення й пошуку всіх клавіш, які треба набрати для слова).

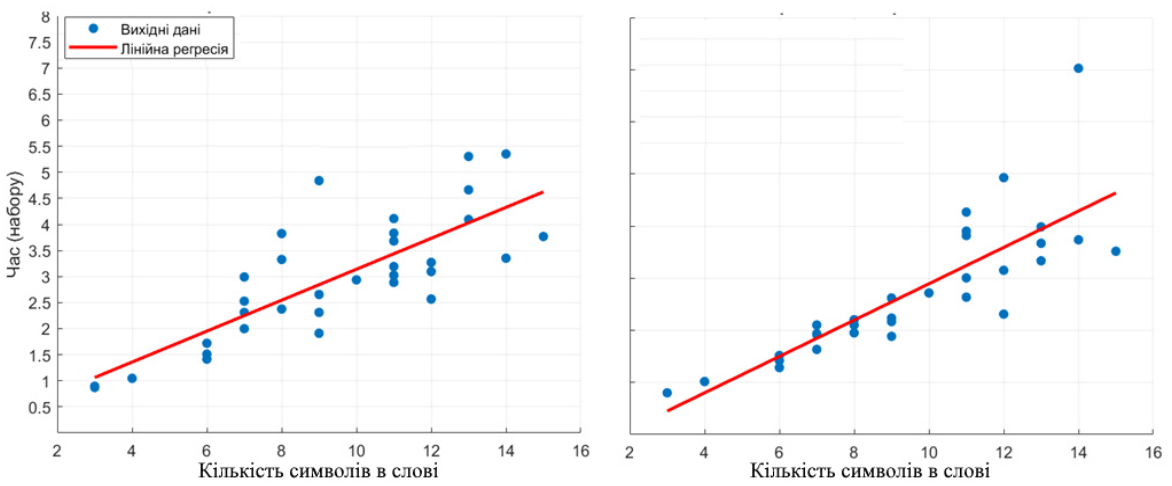


Рис. 10. Узагальнена статистика користувача №1 за залежністю часу набору слово від кількості символів в слові

Бачимо, що закономірність має майже лінійний характер: більше символів – більший час. У випадку, коли присутнє в тестовій фразі декілька різних слів однієї довжини, то вони набираються з різною швидкістю. І хоча в цілому нерівномірність набору слів однакової довжини за часом зберігається, конкретне відхилення може відрізнятись значимо.

У цілому, приходимо до висновку, що час пошуку та час натискання, якщо розглядати їх в інтервалі за різними літерами, дозволяють з високою точністю ідентифікувати стиль набору користувача.

Висновки. Розробка системи біометричної ідентифікації на основі набору тексту, введеного користувачем на клавіатурі, є привабливим рішенням, оскільки не лише потенційно забезпечує надійну ідентифікацію, а й не потребує витрат на спеціальне обладнання. Програмний застосунок, який був розроблений у рамках цієї роботи, дозволяє ефективно проводити процедуру біометричної ідентифікації на основі стилю набору на клавіатурі. Успішне проведення обмежених експериментів з використанням розробленого застосунку підтверджує його ефективність та надійність. Результати експериментів показали ефективність запропонованого критерію, пов’язаного з попаданням при наборі літери в інтервал пошуку та натиснення клавіш еталонного профілю.

Список літератури

1. Giot R, Dorizzi B, Rosenberger C. Analysis of template update strategies for keystroke dynamics. *IEEE Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM '11)*. 2011. P. 21–28.
2. Maisuria L. K, Soon O. C, Kin L. W. Comparison of artificial neural networks and cluster analysis for typing biometrics authentication. *International Joint Conference on Neural Networks.* 1999; P. 3295–3299.
3. Kang P, Hwang SS, Cho S. Continual retraining of keystroke dynamics based authenticator. *Advances in Biometrics, Proceedings.* 2007. V. 4642. P. 1203–1211.
4. Giot R, Dorizzi B, Rosenberger C. Analysis of template update strategies for keystroke dynamics. *IEEE Workshop on Computational Intelligence in Biometrics and Identity Management*. 2011. P. 21–28.
5. Keystroke Deanonymization. URL: https://www.whonix.org/wiki/Keystroke_ Deanonymization
6. Nonaka H, Kurihara M. Sensing pressure for authentication system using keystroke dynamics. *International Conference on Computational Intelligence*. *Istanbul, Turkey*. 2004. P. 19–22.
7. Loy C.C, Lai W.K, Lim C.P. The development of a pressure-based typing biometrics user authentication system. *ASEAN Virtual Instrumentation Applications Contest Submission. National Instruments. Austin., Tex. USA*. 2005.
8. Alshehri A., Coenen F., Bollegala D. Keyboard Usage Authentication Using Time Series Analysis. *18th International Conference on Big Data Analytics and Knowledge Discovery*. 2016. DOI: 10.1007/978-3-319-43946-4
9. Shadman R., Wahab A. A., Manno M., Lukaszewski M., Daqing H. F. H. Keystroke Dynamics: Concepts, Techniques, and Applications. 2303.04605. URL: https://arxiv.org/abs/2303.04605

DEVELOPMENT OF A SOFTWARE APPLICATION FOR BIOMETRIC IDENTIFICATION BY KEYBOARD TYPING STYLE

D.M. Slabenko[1], O.A. Stopakevych[1], A.A. Stopakevych[2]

[1]National Odesa Polytechnic University,
1, Shevchenko Ave, Odesa, 65044, Ukraine
email: stopakevich@op.edu.ua
[2]State University of Intellectual Technologies and Telecommunications
1, Kuznechna, Odesa, 65029, Ukraine
email: stopakevich@gmail.com

This article describes the development of software to identify a user based on his or her keystrokes. Biometric authentication, particularly methods based on behavioral characteristics, is becoming increasingly popular. This is due to its ability to provide security without the need to remember passwords. The development of a biometric identification system based on the typing of a text entered by the user on the keyboard is an attractive solution, as it not only has the potential to provide a fairly reliable identification, but also does not require significant costs for special equipment. This paper discusses parameters that affect typing, including keystroke time, typing speed, error rates, and others that depend on individual user characteristics. The paper also discusses the drawbacks of biometric identification, particularly the impact of external factors such as fatigue or distraction on authentication accuracy. Based on the analysis of parameters, known methods and approaches to biometric identification by keystroke style, a new verification algorithm is proposed. It is based on the analysis of the time intervals between keystrokes and key searches, which allows to determine the correspondence between the stored user profile and the current keystroke. In order to reduce the influence of external factors, the use of a fixed text of at least 300 characters is recommended. The effectiveness of the developed software based on the proposed identification algorithm is confirmed by the results of the experiments conducted with the developed software application. The results show sufficient reliability and accuracy in the identification process. The work is of practical importance for the development of new security methods in information technology and opens new opportunities for the implementation of biometric systems in various fields.

Keywords*:* biometrics, behavioral, identification, authorization, keyboard, typing, user, software, profile, method, algorithm.

DOI 10.15276/imms.v14.no1-2.108
УДК 681.5.01

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 1-2, pp. 108-117

УДОСКОНАЛЕННЯ СИСТЕМИ КЕРУВАННЯ КОНУСНОЮ ДРОБАРКОЮ СЕРЕДНЬОГО ДРОБЛЕННЯ

А.М. Тігарєв[1], Т.Г. Тігарєва[2]

[1]Державний університет інтелектуальних технологій та зв'язку
1, Ковальська вул., м.Одеса, 65029, Україна
email: amtigar@ukr.net
[2] Одеська державна академія будівництва та архітектури
4, Дідріхсона вул., м.Одеса 65029, Україна
email: tatianatigareva@gmail.com

В статті розглядається система автоматизації конусної дробарки середнього дроблення та можливість її удосконалення шляхом використання оптимальної системи керування за допомогою лінійно-квадратичного регулятору з усуненням статичної похибки шляхом введення інтегральної складової. На підставі аналізу існуючих підходів до дробарки як об'єкту керування отримано параметричну схему дробарки. В роботі не розглядається питання щодо регулювання дисперсного складу готового продукту, тому параметрична схема була спрощена з урахуванням перехресних зв'язків між рівнем сировини в дробарці і продуктивністю дробарки. На підставі цього було розроблено її математична модель. З використанням цей моделі дробарки розроблено модель системи керування за каналами, що впливають на рівень сировини в дробарці і продуктивність дробарки. Запропоновано модель оптимальної системи керування дробаркою за допомогою лінійно-квадратичного регулятору з усуненням статичної похибки шляхом введення інтегральної складової. Результати дослідження системи керування при різних комбінаціях збурень показали, що вона є субоптимальною. Це дозволяє застосування такої системи керування для використання в системі автоматизації дробарки, що забезпечить її роботу в оптимальних режимах при різній щільності сировини, а також в значній мірі її безаварійну роботу і зменшення зносу вузлів дробарки.

Ключові слова: конусна дробарка, керування, рівень сировини, продуктивність дробарки, передаточна функція, оптимальна система керування, математичне моделювання, лінійно-квадратичний регулятор.

Вступ. У цей час (в умовах так званого «рваного» виробництва) при відсутності гарантованих замовлень на постачання готового продукту підприємства змушені переглядати свою виробничу політику. Враховуючи постійне зростання цін на енергоносії, сировину, запасні частини та інше, для зменшення витрат на техобслуговування й поточний ремонт підприємства більше уваги приділяють зменшенню зношування й збереженню обладнання. Тому в якості одного із критеріїв зменшення затрат на виробництво товарної продукції починає використовуватися регулювання потужності. Таким чином, розробляється система регулювання потужності дробарки, навіть на шкоду продуктивності. Це дозволяє зменшити зношування обладнання, броньових плит, електроприводів дробарки.

Застосовувані на дробильно-сортувальних заводах і установках щокові або конусні дробарки великого дроблення є головними агрегатами поточно-транспортних систем з переробки матеріалу [1–5]. Єдиним агрегатом потоку, що дозволяє регулювати його продуктивність, є щокова або конусна дробарка первинного дроблення, які оснащені пластинчастим живильником, установленим під ємністю прийомного бункера, що акумулює дроблений матеріал. Завдання автоматизації дробарок середнього дроблення зводиться до підтримки незмінної, за умовами технологічного процесу, продуктивності в поточно-транспортній системі. Тому величина вихідної продуктивності дробарки середнього дроблення може бути використана в якості

параметра керування. Тісний зв'язок між потужністю, що витрачається на дроблення, й пропускною здатністю дробарки, призводить до створення декількох варіантів простого й комбінованого керування з використанням у якості регульованих параметрів потужності (або струму) двигуна подавального транспортеру (ПТ) для підтримання потрібного рівня сировини в дробарці. Контроль ступеня завантаження дробарки здійснюється шляхом підтримання номінального значення рівня в камері дроблення. При підвищенні рівня в камері дроблення потрібно зменшити потужність приводного електродвигуна подавального транспортеру ПТ сировини, у результаті чого знижується подача сировини в камеру дроблення. Це призводить до зменшення рівня сировини в камері дроблення і зменшенню продуктивності дробарки [2–5].

Мета роботи. Метою роботи є розгляд варіанта вдосконалення автоматичної системи, яка забезпечить оптимальне керування конусною дробаркою середнього дроблення для дроблення вапняку при виробництві цементу [6 – 9]. Це дозволить забезпечити роботу дробарки в номінальному режими при підтриманні необхідного рівня сировини в дробарці і забезпечити її номінальну продуктивність, що необхідна для підтримання ритмічної роботи агрегатів, які розташовані на наступних етапах. Тому далі буде розглядатися не загальна система керування дробаркою, а завдання підтримання номінального режиму для зменшення зношування обладнання, броньових плит, електроприводу дробарки.

Матеріали та методи. Існує багато підходів до визначення конусної дробарки, як об'єкта керування й визначення її параметрів [10 – 13]. Більшість авторів вірно визначають параметри, що відносяться до вхідних керуючих впливів, збурень, вихідних вимірювань. Однак, окремі автори допускають грубі помилки. Наприклад, автор [13] відносить до керуючих впливів частоту хитань рухомого конуса, а автор [11] положення конуса, що обертається. Тому слід одразу визначити, що в сучасних конусних дробарках існують тільки три пристрої, якими можливо керувати. До них належать: потужність двигуна дробарки; потужність двигуна транспортеру, що завантажує сировину; пристрої, що змінюють положення конусів дробарки (наприклад, потужність двигуна насосу, якій змінює тиск в гідросистемі, що впливає на положення нижнього конуса або положення кільця, яке регулює зазор між конусами).

У результаті узагальнену параметричну схему дробарки можна представити в наступному вигляді (рис. 1).

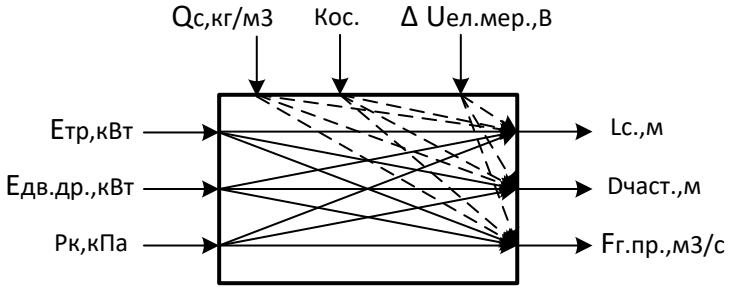


Рис. 1. Узагальнена параметрична схема конусної дробарки, як об’єкту керування

На рис.1: $E_{тр.}$ – потужність транспортеру, що подає сировину в дробарку, кВт; $E_{дв.др.}$ – потужність двигуна дробарки, кВт; $P_к$ – тиск в гідросистемі, що впливає на положення нижнього конуса дробарки, МПа; Lс. – рівень сировини, що завантажена в дробарку, м; $D_{част.}$ – середній діаметр частинок готового продукту, м; $F_{г.пр.}$ – витрата готового продукту, $м^3/с$; $Q_с$ – щільність сировини, $кг/м^3$; $К_{ос.}$ – конструктивні особливості дробарки, $\Delta U_{ел\ мер.}$ – коливання напругі в електричній мережі, В.

Для визначення основних каналів й спрощення системи керування врахуємо, що конусні дробарки для подрібнення сировини для виробництва цементу звичайно

використовуються на другому етапі дроблення, і тому керування дисперсним складом не розглядається, оскільки готовий продукт має значне менший розмір шматків матеріалу і коливання їх розмірів значне менш впливають на подальшу переробку. Крім того, у зв'язку з тим, що сировина (вапняк) не належить до сировини підвищеної твердості, знос броні конусів відбувається досить повільно. Також враховуючі, що конусні дробарки зазвичай працюють в змінному режимі, і згідно з технологічним регламентом перед початком зміни виконуються перевірка стану броні і корегування положення конусів дробарки, то керування положенням конусів для підтримання дисперсного складу продукту на виході конусної дробарки теж не розглядається (таке керування може виконуватися окремою системою керування).

Найбільш прості схеми автоматизації використовують в якості керованого параметра рівень заповнення камери дроблення. При рівності продуктивності живильника й дробарки в режимі, що встановився, рівень заповнення змінюється незначно. У випадку зниження продуктивності дробарки живильник зупиняється або переводиться на знижену швидкість подачі [10 – 12].

На підставі цих міркувань для конусної дробарки середнього дроблення як об'єкта керування можливо вибрати два окремих канали керування: перший канал – «потужність двигуна завантажувального транспортеру – рівень в дробарці»; другий канал – «потужність двигуна дробарки – витрата сировини на виході з дробарки».

Інформацію про рівень сировини в конусній дробарці можливо отримувати за допомогою сучасних мікрохвильових рівнемірів.

У результаті спрощену параметричну схему конусної дробарки можна представити в наступному вигляді (рис. 2).

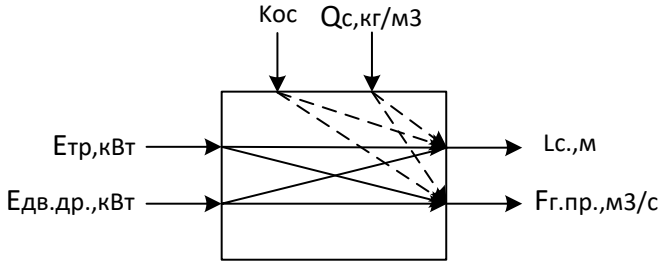


Рис. 2. Спрощена параметрична схема конусної дробарки як об'єкту керування

Основна частина. Для подальшої розробки системи керування розглянемо схему технологічного процесу подрібнення сировини в конусній дробарці середнього дроблення типу КСД-900, яка виготовляється в Україні (рис. 3).

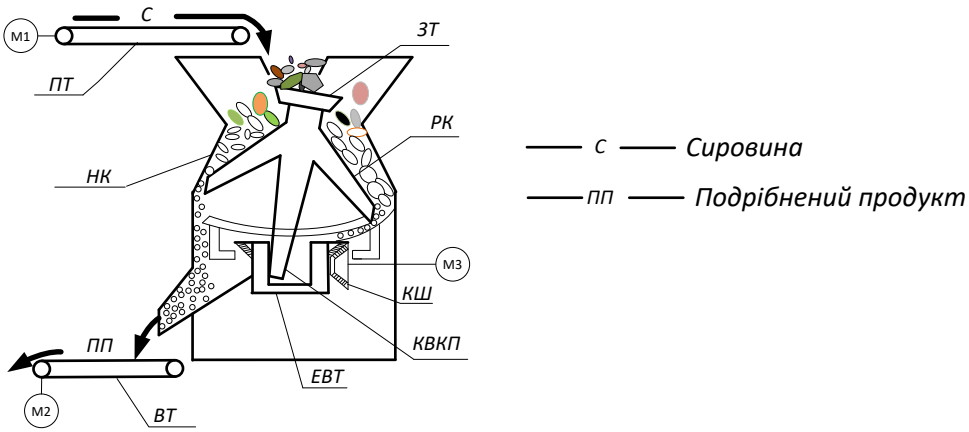


Рис. 3. Схема технологічного процесу подрібнення сировини конусною дробаркою ПТ– подавальний транспортер; КД – конусна дробарка; ВТ – транспортер для вивантаження; ЗТ – загрузочна тарілка; НК – нерухомий конус, РК – конус, що рухається; КШ – конусні шестерні; КВКП – конічний вал конусу, що подрібнює; ЕВТ – ексцентрикова вал-втулка

Технологічними та конструктивними параметрами конусної дробарки КСД-900, які визначають її математичну модель, є [13]: $a_к$=1,5-2,5 – коефіцієнт, що враховує невільне падіння матеріалу в просторі дробарки; $h_к$=2,5 м, – величина шляху падіння від завантажувальної щілини до розвантажувальної, або практично від живильника до датчика витрати готового продукту, м; c_k = 2,0 – безрозмірний коефіцієнт, який для середніх умов при витраті сировини F_c = 0,005м^3/с; n_k = 5,59с$^{-1}$ – частота хитань конуса Основні технічні характеристики пристроїв та режимів, що використовуються при керуванні конусною приведені в табл. 1.

Таблиця 1.

Технічні характеристики пристроїв і режимів для керування конусною дробаркою

Пристрої	Параметри	Режими		
		Мін.	Номін.	Макс.
Двигун подавального транспортеру	Потужність, кВт	2	3,5	5
	Витрата сировини, м^3/с	0,01	0,014	0,02
Двигун дробарки	Потужність, кВт	25	38,5	55
Конусна дробарка	Рівень сировини, м	0,4	0,63	1

Математична модель дробарки має вигляд за каналами:

– потужність двигуна дробарки u1 – витрата готового продукту y1

$$P11 = \frac{0{,}000364}{1{,}05s^2+3{,}35s+1} e^{-4{,}8s};$$

– потужність двигуна дробарки u1– рівень сировини в дробарці y2

$$P12 = \frac{0{,}01638}{9s^2+6s+1} e^{-3{,}2s};$$

– потужність двигуна транспортера u2 – витрата готового продукту y1

$$P21 = \frac{0{,}004}{1{,}05s^2+3{,}38s+1} e^{-4{,}13s}.$$

– потужність двигуна транспортера u2 – рівень сировини в дробарці y2

$$P22 = \frac{0{,}18}{7{,}5s^2+5{,}5s+1} e^{-5s}.$$

З урахуванням уведених позначень на підставі спрощеної параметричної схеми структурну схему математичної моделі дробарки представимо в наступному вигляді (рис. 4).

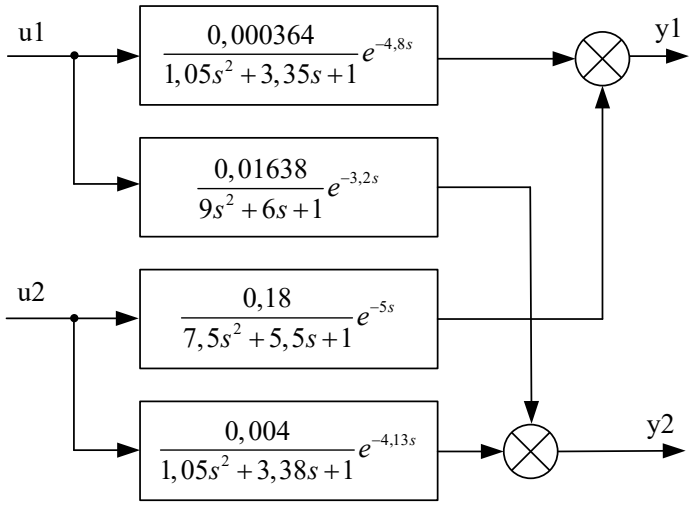


Рис. 4. Математична модель дробарки з урахуванням перехресних зв'язків

Враховуючи наявність перехресних зв'язків між потужністю двигуна дробарки й потужністю транспортера подачі сировини в дробарку, які впливають на витрату готового продукту й рівень сировини в дробарці, для побудови системи керування

дробаркою найкращим є оптимізаційний підхід. У зв'язку з наявністю можливостей у програмному пакеті MATLAB відповідних функцій для побудови оптимальних регуляторів розглянемо можливість застосування лінійно-квадратичного регулятора для його використання при керуванні конусною дробаркою.

Однак враховуючи, що лінійно-квадратичний регулятор є П-регулятором і має значну статичну похибку, виникає необхідність додавання інтегральної складовій для її усунення.

Відомі різні способи реалізації цього підходу [14 – 17]. Більшість із них мають різні недоліки, які у першу чергу обумовлені неточністю моделі об'єкта, його нелінійністю, зміною його параметрів у часі та інші. Відомо, що в неперервному часі математична форма запису в вигляді простору станів не дозволяє представити чисте запізнення без апроксимації – частіше за все обирають апроксимацію Паде першого порядку [14]. Для синтезу цифрового регулятора переведемо математичну модель з неперервного в дискретний час (назвемо таку дискретну модель Pd_2). Цифрова система керування з лінійно-квадратичним регулятором має включати спостерігач стану й модель збурень в вигляді стрибку (інтегратор). В літературі описані дві структури систем автоматичного керування: з відновленням та без відновлення станів моделі збурення (вони і так відомі) [14]. Для реалізації виберемо систему без відновлення станів моделі збурення.

Розробка моделі керуванням з використанням лінійно-квадратичного регулятору в програмному пакеті MATLAB виконана в наступній послідовності.

1. Апроксимуємо запізнювання в МПФ ланкою 1 порядку.

2. Переводимо перетворену МПФ в простір станів в неперервному часі.

3. Виконуємо дискретизацію систем і отримуємо дискретну систему Pd_2 {A, B, C, D} в просторі станів з кроком дискретності 1 с.

4. Введемо значення вагових коефіцієнтів Q_{1K1}, Q_{1k2}, Q_{1L}, R_{1K}, R_{1L}.

Для початку доцільно їх прийняти одиничними.

5. Сформуємо вагові матриці: $Q_1 = \begin{bmatrix} C^T \cdot Q_{1K1} \cdot C & 0 \\ 0 & Q_{1K2} \end{bmatrix}$, $R_1 = R_{1K}$

6. Розрахуємо регулятор стану з інтегральною складовою за допомогою функції $K=lqi\ (P_{d2}, Q_1, R_1)$.

Ця функція використовує розширену матрицю моделі виду (I – одинична матриця).

$$A_1 = \begin{bmatrix} A & 0 \\ -C \cdot \Delta t & I \end{bmatrix},\ B_1 = \begin{bmatrix} B \\ -D \cdot \Delta t \end{bmatrix}.$$

7. Сформуємо наглядач стану за допомогою функції *dlqr* для матриць системи P_{d2}

$$L = dlqr\left(A^T, C^T, Q_{1L}, R_{1L}\right)^T.$$

8. Сформуємо регулятор C_1, як систему в дискретному просторі станів зі спостерігачем за допомогою команд $L = estim\left(P_{d2}, \mathrm{L}, [1:m]\right)$, $C_1 = lqgtrack\left(L, K\right)$,

де $m = 2$ – кількість входів й виходів.

Моделювання перехідних процесів ведеться за допомогою пакету візуального імітаційного моделювання Simulink. При моделюванні розроблений цифровий регулятор підключимо до моделі в неперервному часі. Зовнішній вигляд схеми розробленої системи керування дробаркою за обраними каналами в програмному пакеті Simulink має наступний вигляд (рис. 5).

Основним збуренням при роботі конусної дробарки при виробництві цементу є щільність вапняку, яка складає 2700-2900 кг/м^3, тобто може коливатися в межах ≈ ± 100 кг/м^3 або 3.6%. При підвищенні щільності вапняку для дроблення шматка потрібна більша потужність двигуна дробарки й при цьому час перебування шматка в дробарці

зростає. При цьому спадає продуктивність дробарки. При використанні сировини навіть із одного з кар'єру залежність співвідношення сировини підвищеної твердості й меншої твердості невідома. Тому завжди спостерігається коливання потужності двигуна транспортеру і двигуна дробарки і відповідно її продуктивності.

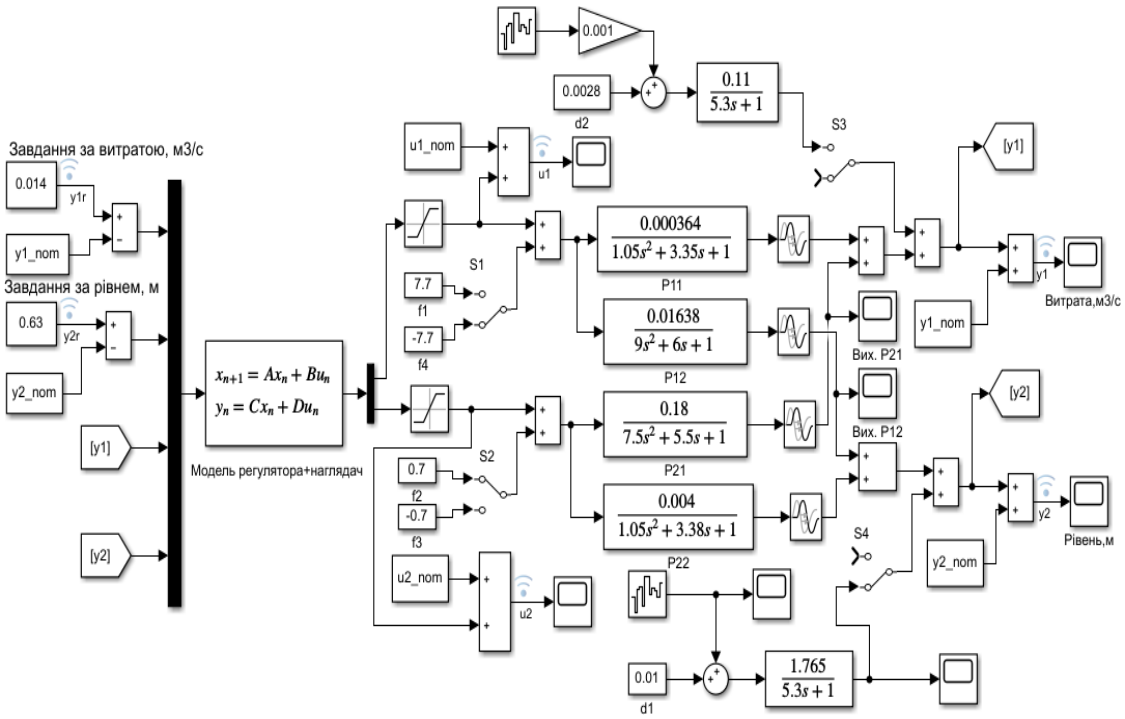


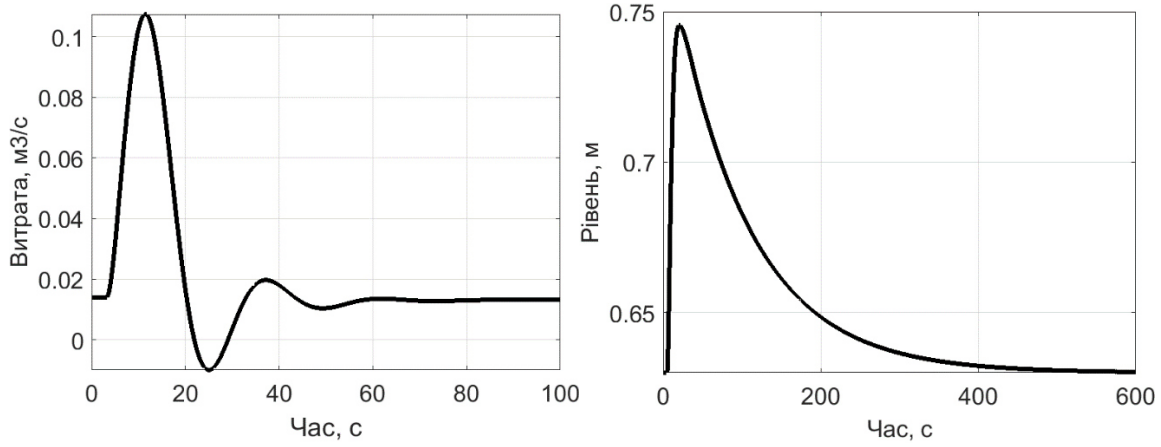
Рис. 5. Модель системи регулювання рівня сировини в дробарці і продуктивності дробарки за готовим продуктом

Припускаючи, що ці коливання підкоряються нормальному закону розподілу, представимо модель збурювань у вигляді послідовного з'єднання генератора білого шуму Band-Limsted White Noise і аперіодичної ланки першого порядку.

Припускаючи, що залежність між продуктивністю дробарці, рівнем сировини і щільністю вапняку має лінійну залежність, тоді модель збурювань обома каналами: подачі сировини і продуктивності дробарки буде мати аналогічну структуру. На підставі цих міркувань виконано дослідження впливу щільності сировини шляхом подачі сигналів збурень на виходи відповідних каналів.

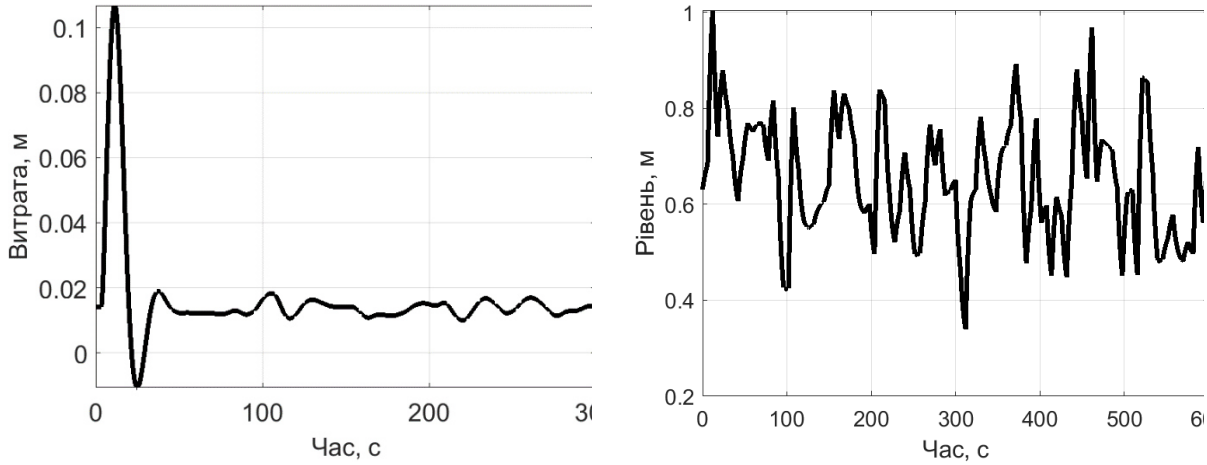
На підставі експериментальних відомостей, що приведені в [18] і описують часові реалізації ширини розвантажувальної щілини і потужності електроприводу дробарки, які виміряні у процесі дроблення руди, вважаємо, що вони аналогічно характеризують і часові коливання потужності дробарки і завантажувального транспортеру. На підставі цих відомостей була вибрана частота коливань ≈0,3-0,4 Гц, а максимальне відхилення амплітуди коливань ≈ 20% від продуктивності дробарки і рівня сировини визначено параметри налаштування генератора білого шуму при побудові моделі цих збурень. Для забезпечення можливості підключення цих моделей до системи керування передбачені перемикачі S3 і S4.

При моделюванні були проведені дослідження при всіх можливих комбінаціях, і визначено, що система керування забезпечує роботу дробарки в припустимих межах. Найгіршими комбінаціями збурень при роботі дробарки будуть максимальний щільність сировини і максимальна потужність двигуна дробарки. Перехідні процеси системи керування приведені на рис. 6 та 7.



а *б*

Рис. 6. Перехідні процеси зміни витрати готового продукту (*а*) та рівня сировини в дробарці (*б*) при завданнях *y1r, y2r* і найгіршій комбінації збурень з ключами S1–S2.



а б

Рис. 7. Перехідні процеси зміни витрати готового продукту (*а*) та рівня сировини в дробарці (*б*) при завданнях *y1r, y2r* і найгіршій комбінації збурень з ключами S3–S4.

Аналіз перехідних процесів показує, що запропонована система керування є сталою. Крім того, результати моделювання показують, що навіть при найгірших комбінаціях збурень відхилення продуктивності і рівня сировини в дробарці не перевищують заданих значень.

Висновки. Запропонована метод удосконалення система керування конусною дробаркою середнього дроблення, що використовується для дроблення вапняку при виробництві цементу. Проведено аналіз дробарки, як об’єкту керування. На підставі спрощеної параметричної схеми конусної дробарки як об’єкту керування, запропоновано математичну модель дробарки з урахуванням перехресних зв'язків між каналами. Виконано розробку моделі оптимальної системи керування дробаркою КСД-900 Харківського заводу промислового обладнання «ПРОГРЕС» з застосуванням цифрового лінійно-квадратичного регулятору з інтегральною складовою в програмному пакеті MATLAB-Simulink. Проведено моделювання системи при різних збуреннях. Визначено, що запропонований підхід робить систему керування квазіоптимальною. Розроблена система керування забезпечує підтримання завдань за потужністю двигуна дробарки и рівнем сировини в межах ±20% відхилень керуючих впливів, що обумовлено коливанням щільності сировини. Також потужність двигуна дробарки і двигуна транспортеру не перевищує максимальне допустимих значень. Це дозволяє рекомендувати запропоновану систему керування для застосування при розробці промислових систем

керування конусною дробаркою середнього дроблення для дроблення вапняку при виробництві цементу.

Список літератури

1. Андреев С. Е., Перов В. А., Зверевич В. В. Дробление, измельчение и грохочение полезных ископаемых. Москва : Недра, 1980. 415 с.
2. Пивняк Г.Г., Вайсберг Л.А., Кириченко В.И., Пилов П.И., Кириченко В.В. Измельчение. Энергетика и технология. Москва : Руда и металлы, 2007. 296с.
3. Оборудование для переработки сыпучих материалов: учебное пособие / В.Я. Борщев, Ю.И. Гусев, М.А. Промтов, А.С. Тимонин. Москва : Машиностроение-1», 2006. – 208 с.
4. Линч А.Дж. Циклы дробления и измельчения. Моделирование, оптимизация, проектирование и управление. Москва : Недра, 1981. 343 с.
5. Воробьев Н. И., Новик Д.М. Обогащение полезных ископаемых. Минск : БГТУ, 2008. 174 с.
6. Цементні заводи України URL : https://energosteel.com/cementnye-zavody-ukrainy/
7. Сировинна база для виробництву цементу URL: https://www.karer.in.ua/ limestones.php
8. Види вапняків URL: https://www.voscem.ru/articles/cement-material/ karbonat/
9. Вапняк технічні характеристики URL: https://www.karer.in.ua/limestones.php
10. Олейников В. А., Тихонов О. Н. Автоматическое управление технологическими процессами в обогатительной промышленности. Москва : Недра, 2006. 355 с.
11. Троп А. Е., Козин В.З., Прокофьев Е.В. Автоматическое управление технологическими процессами обогатительных фабрик: технический справочник. Москва : Недра, 1986. 303 с.
12. Марюта А.Н., Качан Ю.Г., Бунько В.А. Автоматическое управление технологическими процессами обогатительных фабрик. Москва : Недра, 1983. 277 с.
13. Комаров А.Я., Прокофьев Е.В. Аналитическое определение параметров статических и динамических характеристик щековых и конусных дробилок: *Известия Уральской государственной горно-геологической академии. Серия: Горная электромеханика*. 1997. Вып. 6. С. 181-189.
14. Стопакевич А.А. Системный анализ и теория сложных систем управления. Одесса : Астропринт, 2013. 352 с.
15. Di Ruscio D. Discrete LQ optimal control with integral action: A simple controller on incremental form for MIMO systems. *Modeling, Identification and Control.* 2012. V. 33. No. 2., P. 35-44.
16. Anderson B. D. O., Moore J. B. Optimal Control: Linear Quadratic Methods. Prentice-Hall International Editions, 1989.
17. Johansson K. H. Interaction bounds in multivariable control systems. *Automatica*. 2002. V.38. No.2. P. 1045–1051. DOI:10.1016/S0005-1098(01)00285-0
18. Михайленко О.Ю., Щокін В.П., Федоренко П.Ю. Аналіз впливу ширини розвантажувальної щілини на споживання електричної енергії конусної: *Вісник Криворізького національного університету*. 2013. Вип. 34. С. 57-61.

IMPROVEMENT OF THE MEDIUM CRUSHER CONE CONTROL SYSTEM

A.M.Tigarev[1], T.G. Tigareva[2]

[1]State University of Intellectual Technologies and Communications
1, Kovalska st., Odesa, 65029, Ukraine
email: amtigar@ukr.net
[2]Odesa State Academy of Civil Engineering and Architecture
4, Didrichson st., Odesa, 65029, Ukraine
email: tatianatigareva@gmail.com

The article discusses the control system of the cone crusher of medium crushing and the possibility of its improvement. Based on the analysis of the existing approaches to the crusher, the parametric scheme of the crusher is obtained as a control object. The work does not address issues related to the regulation of the dispersed composition of the finished product. Therefore, the parametric scheme was simplified taking into account the cross-links between the level of raw materials in the crusher and the capacity of the crusher. Based on this, it mathematical model was developed. A model of an optimal crusher control system using a linear-quadratic regulator with elimination of static error by introducing an integral component is proposed. The results of the study of this model with different combinations of perturbations showed that it is suboptimal. Thus, this will allow the use of such a control system to automate the crusher, which will provide its work in optimal modes at different density of raw materials, as well as to a large extent ensure its accident-free operation and reduce wear of the crusher units.

Keywords: cone crusher, control, raw material level, crusher capacity, transfer function, optimal control system, mathematical modeling, linear-quadratic regulator.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 14, номер 1-2, 2024. Одеса – 118 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 14, номер 1-2, 2024. Одесса – 118 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 14, No. 1-2, 2024. Odesa – 118 p.

Засновник: Національний університет «Одеська політехніка»

Зареєстровано Міністерством юстиції України 04.04.2011р.
Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Національного університету «Одеська політехніка», (протокол №10 від 27.03.2024р.)

Адреса редакції: Національний університет «Одеська політехніка»,

1, Шевченка проспект, Одеса 65044 Україна

Web: www.immm.op.edu.ua (immm.opu.ua)

E-mail: immm.ukraine@gmail.com