# Development of a Biometric Electronic Signature based on Iris Features*

Nazar Oleksiv[1,†] and Mariia Nazarkevych[1,*,†]

[1] Lviv Polytechnic National University, 12 Stepan Bandera str., 79000 Lviv, Ukraine

**Abstract**

This paper presents a novel approach to ensuring secure identification in cyberspace by utilizing a biometric electronic signature generated from the unique features of the human iris. The proposed technology combines the high reliability of biometric data with modern cryptographic methods, creating a robust authentication mechanism resistant to attacks. The study addresses key aspects of generating cryptographic keys from biometric data, analyzing the system's resilience against forgery and compromise, and integrating the technology with existing electronic signature standards. Special attention is given to user convenience—eliminating the need to remember complex passwords—and to challenges related to privacy and the protection of biometric data. The results demonstrate the potential of the developed technology for both individual users and corporate or government sectors, offering new opportunities for cybersecurity and contactless identification.

**Keywords**

biometric electronic signature, iris recognition, secure identification, cryptographic key, data protection, authentication, contactless identification

## 1. Introduction

In the modern world, where cybersecurity is critically important for protecting personal and corporate data, traditional authentication methods such as passwords and tokens no longer meet the security and convenience requirements. The increasing number of cyber threats and attacks, such as phishing and password compromise, raises concerns about the effectiveness of conventional protection methods. As a result, there is a growing need for new approaches to authentication and digital signatures that can provide a higher level of security without compromising user convenience [1].

One such innovative approach is the use of biometric data, specifically the iris, to create an electronic signature. The iris is a unique biometric characteristic, making it nearly impossible to forge [2, 3]. Due to its uniqueness and stability, the iris can serve as a reliable basis for authentication and electronic signature generation, offering a new level of security compared to traditional methods.

The goal of this paper is to develop and present a technology that uses biometric iris features to generate an electronic digital signature. The proposed approach combines modern cryptographic methods with biometric data to create a robust authentication system resistant to attacks [4, 5]. A significant advantage of this technology is the elimination of the need to remember passwords or use hardware tokens, significantly enhancing user convenience.

The novelty of this research lies in the integration of biometric technologies with electronic signatures to create a secure authentication mechanism that can be used across a wide range of applications—from individual users to large corporate and government entities. Key aspects of this approach include the protection of biometric data privacy, the reliability of signature generation algorithms, and ensuring compatibility with existing electronic signature standards and Public Key Infrastructure (PKI).

* CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

nazar.oleksiv.mnsa.2020@lpnu.ua (N. Oleksiv); mariia.a.nazarkevych@ lpnu.ua (M. Nazarkevych)

0000-0001-7821-3522 (N. Oleksiv); 0000-0002-6528-9867 (M. Nazarkevych)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

CEUR-WS.org/Vol-3991/paper4.pdf

This paper explores the possibilities and prospects of implementing biometric electronic signatures, providing theoretical justification and experimental results that demonstrate the effectiveness of the proposed approach. The study also addresses issues of security, user convenience, and legal compliance of biometric electronic signatures in the context of modern cybersecurity requirements.

## 2. Literature and technology overview

This section examines modern approaches to biometric authentication, and electronic signature technologies, and analyzes the existing challenges in the field of cybersecurity and personal data protection. A review of current publications provides an understanding of the theoretical foundation and technological limitations faced by contemporary security systems.

### 2.1. Drawbacks of digital signatures

Digital signatures are one of the key technologies for ensuring the authenticity, integrity, and security of data. They are widely used in electronic document circulation, online transactions, and other digital systems. However, despite their popularity, digital signatures have some drawbacks and limitations that impact their effectiveness and security.

Types of digital signatures and their vulnerabilities Digital signatures can be broadly classified into the following types:

*Simple Electronic Signatures (SES)*—used for basic authentication, such as attaching a scanned image of a signature to a document. They do not provide cryptographic protection and can be easily forged.

*Advanced Electronic Signatures (AES)*—utilize cryptographic methods to verify authenticity, but require strong protection of keys, which can be stolen or compromised.

*Qualified Electronic Signatures (QES)* - meet the highest security standards but require a complex infrastructure, including certificates from trusted Certification Authorities (CAs). Their cost and the complexity of integration into systems can limit their use.

Drawbacks of digital signatures dependence on private keys: the security of a digital signature largely depends on the private key. If it is compromised, malicious actors can forge the signature without the owner's knowledge.

Issues with Owner Authentication: a digital signature verifies the correctness of the key but does not provide physical identification of the owner. This means that third parties who have gained access to the key can impersonate another user.

Phishing and Social Engineering Risks: users may be tricked into providing access to their keys or certificates, making them vulnerable to fraudulent activities.

Technological Implementation Flaws: there are cases where weak cryptographic algorithms or system implementation errors have created vulnerabilities for attacks. For instance, using outdated algorithms such as MD5 or SHA-1 is risky due to the possibility of hash collisions.

High Dependence on Infrastructure: digital signatures require a complex infrastructure, including Certification Authorities (CAs), Registration Authorities (RAs), and certificate verification mechanisms (OCSP, CRL). Failures or compromises in this infrastructure can lead to the loss of access to signatures or trust in them.

Real-World Examples of Drawbacks Document Forgery: In 2020, instances were reported where counterfeit digital signatures were used in banking transactions, with attackers gaining access to private keys through phishing. Another example, the SHA-1 vulnerability was exploited to create two different documents with the same digital signature, undermining the trust in signatures as a method for ensuring data integrity.

### 2.2. Biometric Authentication

Biometric authentication is one of the most promising methods for ensuring security in today's world. It is based on unique physiological and behavioral characteristics of individuals, such as

fingerprints, facial recognition, voice, or iris patterns. The main advantages of biometric authentication lie in its high accuracy and convenience for users, as it eliminates the need to remember complex passwords or PINs. Unlike traditional authentication methods, biometric systems rely on distinctive traits specific to an individual, making it impossible to forget or lose them.

Key biometric characteristics used for authentication:

*Fingerprints.* One of the oldest and most widely used biometric parameters. Fingerprint-based systems are known for their accessibility and ease of use; however, they have certain limitations. For example, fingerprints can be altered due to injuries or diseases, which may reduce the accuracy and reliability of the system. Additionally, there is a risk of forgery using technologies such as fake fingerprints or "silicone fingerprints" [6].

*Face recognition.* Technologies have become widely used due to their convenience and ability to perform remote identification. Algorithms for face recognition analyze features such as the shape of the nose, lips, eyes, and the distance between them. However, these systems also have some drawbacks: they may be less effective under different lighting conditions or when faces are obscured by masks or other coverings [7].

*Iris recognition.* Unique part of the human eye that does not change throughout life and is distinctive for each person. Iris recognition is highly accurate due to the large number of fine details that are difficult to forge. It is also resistant to external factors like lighting and can be used even in certain physical conditions, such as wearing glasses or contact lenses [8].

*Voice recognition.* Use specific acoustic features unique to each individual, such as frequency, pitch, and timbre of the voice. Although this method is convenient, it has its limitations, as the voice can be forged using synthesizers, and certain physical conditions (e.g., illness, hoarseness) may reduce recognition accuracy [9].

Moreover, biometric authentication methods, such as iris scanning, offer a significantly higher level of security. All biometric traits, such as iris structure, facial features, and fingerprints, are unique to each individual, making them nearly impossible to forge or replicate. This makes them a reliable tool for identity verification, as users attempting to perform transactions must physically present themselves. Furthermore, these systems greatly reduce the chances of fraud, as even if attackers have a photo or fingerprint of a person, they cannot replace a live individual.

Another key advantage of biometric authentication is its ability to integrate seamlessly into various technological platforms. From smartphones to corporate access systems, biometric systems can enhance the convenience and efficiency of user interactions. They allow for quick authentication without requiring additional actions from the user, which is especially valuable in an era of rapid technological advancements.

All of these factors make biometric authentication more effective compared to traditional security methods, offering high levels of security, ease of use, and reduced fraud risk. As a result, this method has become an essential tool in many sectors, including financial transactions, access to sensitive information, and the protection of personal data.

Technologies used in biometric authentication involve several key processes. The main step in biometric systems is the collection and processing of images or data related to biometric features. In the case of iris recognition, algorithms apply image processing techniques to extract crucial features, such as the texture of the iris and its geometric characteristics [10]. To ensure high accuracy, machine learning methods, particularly neural networks, are often employed, as they are well-equipped to handle large volumes of data and deliver precise recognition.

For each biometric parameter, unique characteristics must be extracted from the collected images to be used for comparison. In iris recognition, these characteristics may include texture elements, color, and the shape of patterns found in the iris, along with their distribution across the iris. Algorithms use filtering and detection methods to identify these features, helping to mitigate the impact of challenges like poor lighting or changes in position [11].

Modern biometric systems also rely heavily on machine learning techniques to enhance both the accuracy and speed of authentication. The use of deep neural networks and other artificial

intelligence methods greatly improves the efficiency of identification, particularly when working with complex features like the iris or voice [12]. These techniques allow the system to adapt automatically to new conditions, thus improving its overall recognition capabilities.

## 2.3. Electronic Signatures and Cryptography

Electronic signatures (e-signatures) are a technological solution that allows for the verification of the signer's identity and ensures the integrity and authenticity of electronic documents. By using an electronic signature, a user can be identified, the act of signing the document can be confirmed, and the document can be protected from alterations after it has been signed (Fig. 1). One of the key aspects of an electronic signature is its cryptographic foundation, which provides a high level of security and plays a vital role in protecting against fraud and forgery.

This document's hash is then signed with the signer's private key, creating a unique signature for the specific document.

The recipient of the document can verify the signature using the corresponding public key and ensure that the document has not been altered after signing.

Hashing is the process of creating a unique, fixed-size value (hash) from data of arbitrary size. Hash functions like SHA-256 or SHA-3 ensure data integrity because even a minor change in the input data results in a significant change in the hash. In the context of electronic signatures, hashing is a critical step for verifying the integrity of the signed document [13].

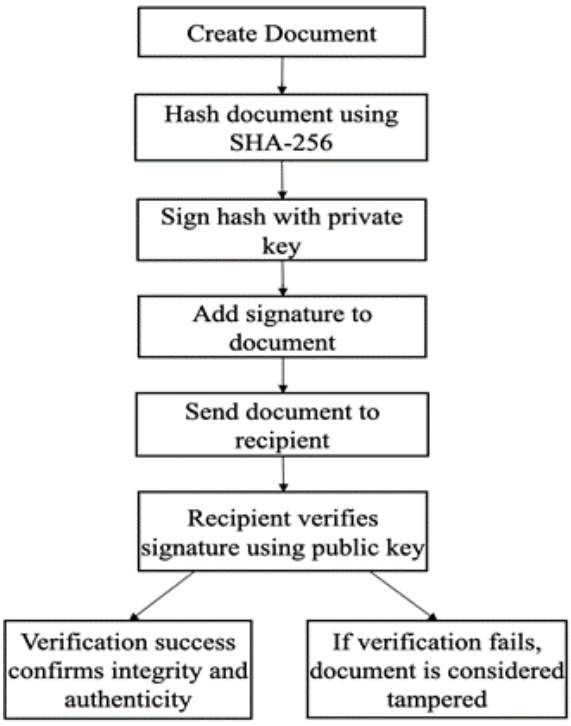


**Figure 1:** Creation Process of an Electronic Digital Signature (EDS)

Digital certificates are used to validate the authenticity of an electronic signature. This certificate is an electronic document that contains the signer's public key and other information about them, such as details about the issuing authority. Digital certificates are typically issued by certification authorities (CAs), which verify the signer's identity, thus establishing trust in the signature.

In the case of biometric signatures, such as using the iris for signing, the basic process remains similar, with the addition of a new step—capturing and processing biometric data.

The generation of a biometric signature involves:

First, the user scans their iris using a specialized sensor or camera capable of capturing a high-resolution image of the eye. Based on the acquired images, algorithms are applied to extract unique

features of the iris, such as texture, color characteristics, and the geometric properties of patterns found in the iris. These characteristics are transformed into a biometric template, which is then cryptographically protected. The template is passed through a hash function to create a unique hash that is signed with the private key.

The biometric template can be integrated with existing cryptographic systems. In this case, the signer uses their private key to sign the document, along with the biometric data. Since biometric data is unique to each individual, it can serve as an additional layer of protection when forming the signature.

Regarding security, using biometric features for creating an electronic signature is more reliable because these features are unique and cannot be transferred or forged in the same way passwords or PIN codes can be. However, it is crucial to protect biometric data during the collection, storage, and transmission phases. Typically, this is done by encrypting the biometric data using modern cryptographic algorithms, which reduces the risk of theft or forgery.

In electronic communications between companies, government agencies, and clients, the use of electronic signatures significantly simplifies the processes of signing contracts and agreements, reducing the need for personal presence to sign paper documents. In a legal context, an electronic signature provides a document with the same legal force as a handwritten signature on paper.

In the healthcare sector, electronic signatures can be used to sign medical records, patient histories, prescriptions, and other documents, enhancing the efficiency and security of medical processes.

For providing government services, such as tax filings, property registration, or submitting various applications, electronic signatures enable processes to be carried out online without the need to visit government offices.

## 2.4. Challenges and Limitations of Biometrics in Cybersecurity

Biometric technologies offer a high level of security due to the unique and stable nature of biometric data, such as fingerprints or iris patterns [14]. These features make them more reliable than traditional passwords or PIN codes, which can easily be forgotten or stolen. However, the irreversible nature of biometric data poses a significant drawback, as it cannot be replaced if compromised [15].

One of the primary concerns with biometrics is ensuring data privacy. If biometric information is accessed by unauthorized parties, it could be exploited for fraud or identity theft. Regulations like the GDPR impose strict requirements for handling such sensitive data [16].

Technical and hardware constraints also present notable challenges. Low-quality or budget sensors may produce errors, potentially allowing unauthorized access or denying entry to legitimate users. Moreover, factors such as aging, medical conditions, or physical injuries can impact the accuracy of biometric systems [17].

Another critical issue is the risk of biometric data forgery. Advanced technologies, such as 3D printing or high-resolution photography, can be used to create counterfeit biometric data. Attackers may also target databases where biometric templates are stored, posing a serious security threat [18].

Social perceptions further complicate the adoption of biometric systems. Many users are wary of these technologies, citing concerns about privacy and the potential for continuous surveillance. To gain public trust, it is crucial to ensure transparency in how biometric data is used and managed [19].

Despite these challenges, biometrics remains a promising avenue for enhancing cybersecurity. The successful adoption of biometric systems will depend on advancing the underlying technologies, mitigating associated risks, and establishing clear and comprehensive regulatory frameworks.

### 2.5. Prospects of Using Iris Patterns for Generating Electronic Signatures

The human iris is a distinctive and stable biometric feature that provides a promising foundation for innovative approaches to electronic authentication and signing. Unlike other biometric traits such as facial features or fingerprints, the structure of the iris remains unchanged over time, making it a highly reliable option for generating electronic signatures [20]. This inherent uniqueness allows for the creation of secure systems that eliminate the need for traditional passwords or PIN codes, which are often susceptible to breaches.

The exceptional accuracy of iris recognition makes it an ideal choice for forming digital signatures, enabling seamless automatic identification and fostering greater trust in electronic transactions. When compared to conventional methods like passwords or smart cards, iris-based biometric authentication offers notable benefits, including higher precision, reduced susceptibility to errors and fraud, and the elimination of risks associated with forgotten credentials or stolen data [21, 22].

At the same time, there are technical hurdles to overcome. Effectively using the iris as a basis for electronic signatures requires advanced scanners and specialized software capable of processing and securely storing biometric templates. Additionally, robust measures must be in place to protect biometric data, as any breach or theft could have serious implications for users' security [23, 24].

Despite these challenges, progress in biometrics and cryptography suggests a bright future for using iris-based systems in generating electronic signatures. Such advancements pave the way for enhanced security and convenience across various domains, from financial transactions to government services [25, 26].

In conclusion, integrating the iris as a key element of electronic signatures holds the potential to redefine cybersecurity practices. This approach promises not only heightened security but also a more user-friendly experience compared to traditional authentication methods.

## 3. Methodology

The methodology presented in this work outlines the key stages of designing and implementing a biometric electronic signature based on iris recognition. The proposed approach incorporates the specifics of biometric technologies, cryptographic algorithms, integration with modern Public Key Infrastructure (PKI) standards, and security measures to ensure data protection [27].

### 3.1. Image Processing

The process of iris biometric analysis begins with image capture using a smartphone camera. Modern smartphones are equipped with high-quality cameras and support for infrared (IR) illumination, enabling clear image acquisition even under challenging lighting conditions.

Preprocessing of the iris image is a critical stage that ensures the quality of subsequent analysis. This step involves methods aimed at enhancing contrast, reducing noise, and extracting key details necessary for accurate recognition.

The algorithm specifies a minimum resolution of 512×512 pixels to ensure enough detail of the iris texture. While PNG or JPEG formats are commonly used, images are often converted to grayscale during preprocessing to simplify analysis [28, 29]. If the smartphone supports IR filters, it helps mitigate the effects of glare and color artifacts, enhancing the overall image quality.

The captured image is then transmitted to a server for further processing, ensuring that advanced computational resources can be applied for segmentation, feature extraction, and template generation (Fig. 3). This approach leverages the capabilities of mobile devices while maintaining the accuracy and efficiency of the biometric analysis process [30].

On the server side, the first step is converting the image to grayscale, which significantly reduces processing complexity. The conversion formula is based on weighted coefficients of the primary colors (red, green, and blue):

$$Y = 0{,}2989\,R + 0{,}587\,G + 0{,}114\,B \tag{1}$$

where RRR, GGG, and BBB are the intensities of the red, green, and blue channels, respectively. This formula preserves the brightness of the image and simplifies the analysis of textural characteristics.

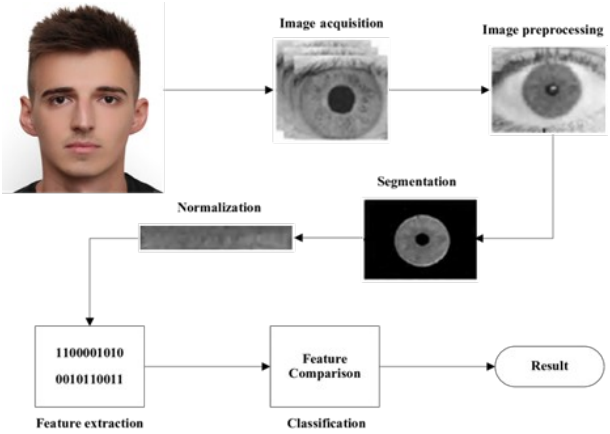


**Figure 2:** The process of iris processing

**Figure 3:** Image greyscale

Noise suppression is performed next using a Gaussian filter, which smooths out minor artifacts. The Gaussian kernel function is defined as:

$$G(x, y) = \frac{1}{2\pi\sigma^2} e^{\frac{-x^2+y^2}{2\sigma^2}} \tag{2}$$

where $\sigma$is the standard deviation controlling the degree of blurring. For experiments, $\sigma$=1.55 is recommended, providing an optimal balance between noise removal and edge preservation [27].

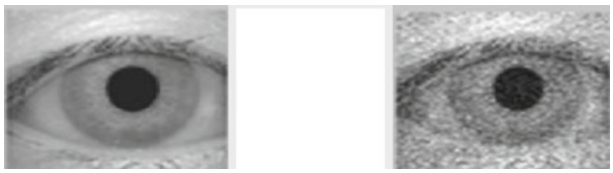

**Figure 4:** Gaussian filter

Contrast equalization is performed using adaptive histogram equalization (CLAHE). This method divides the image into small blocks and equalizes the histogram of each block individually. The approach enhances details even in dark or overexposed regions of the iris. The whole algorithm process is illustrated schematically in Fig. 5.

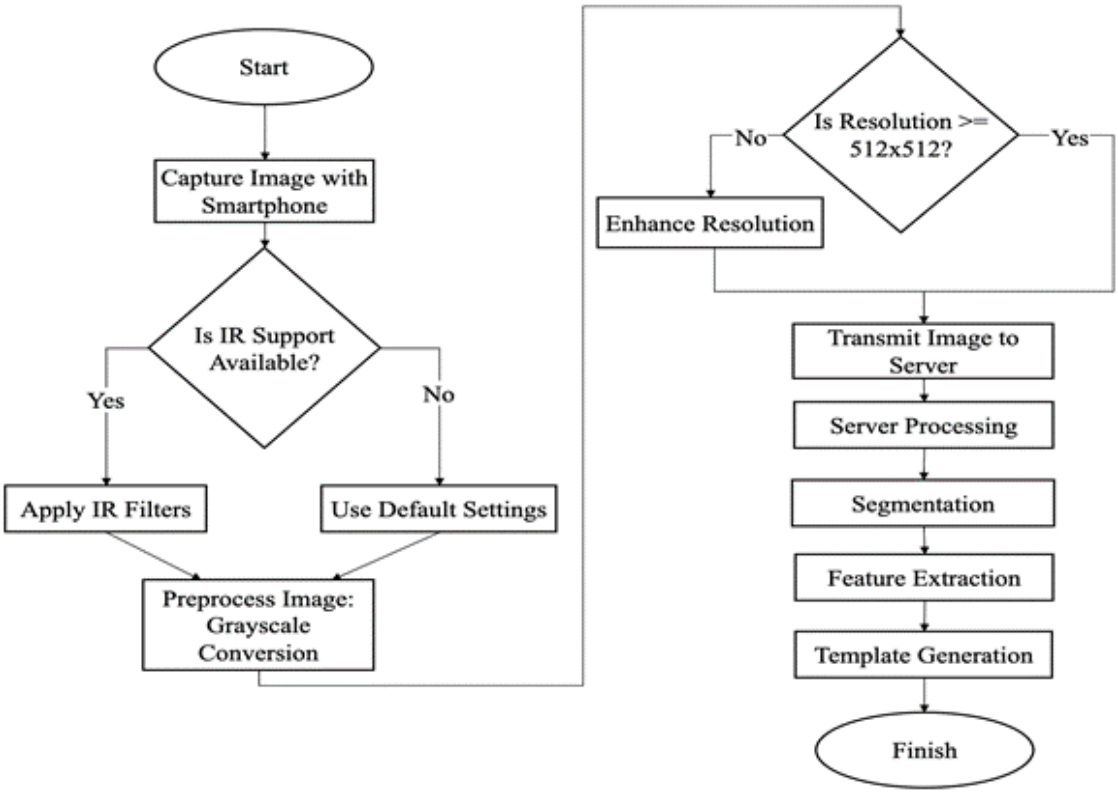


**Figure 5:** Algorithm flowchart

### 3.2. Cryptographic Key Generation

The generation of a cryptographic key based on iris biometric data is a central component of the proposed methodology. The primary goal is to derive a unique and secure key that can be used for creating a digital signature without the need to store raw biometric data.

The cryptographic key generation process consists of several stages:

*Feature Extraction.* After the preprocessing stage (Step 3.1), unique features of the iris are extracted. This process employs Gabor filters, which are effective in capturing the textural characteristics of the image. A Gabor filter is mathematically defined by the following function:

$$G(x, y; \lambda, \theta, \psi, \sigma, \gamma) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right)\cos\left(-2\pi\frac{x'}{\lambda} + \psi\right) \quad (3)$$

where $x' = x\cos\theta + y\sin\theta$, $y' = -x\sin\theta + y\cos\theta$

Parameters of the function:

- $\lambda$: Controls the scale of the filter.
- $\theta$: Determines the direction of the filter.
- $\psi$: Adjusts the phase of the sinusoidal wave.
- $\sigma$: Defines the extent of the Gaussian envelope.
- $\gamma$: Controls the ellipticity of the filter.

This function is applied to the grayscale iris image, identifying fine details such as ridges, crypts, and furrows. The extracted features are represented as a compact vector of numerical values, capturing the unique structure of the iris. These feature vectors serve as the foundation for generating a biometric template, ensuring reliable identification [31, 32].

*Feature Encoding.* The extracted features are encoded into a binary iris code of 512 bits, ensuring a high degree of uniqueness for identification. The encoding process involves discretizing the feature vector and transforming it into a format suitable for cryptographic applications.

This binary representation captures the unique texture of the iris in a compact and standardized form, making it both efficient for storage and robust against variations in imaging conditions. The resulting iris code serves as a secure input for cryptographic key generation and further biometric verification processes.

*Key Generation.* A cryptographic key is generated from the binary iris code using an expansion algorithm.

The SHA-256 algorithm is a cryptographic hash function that generates a 256-bit hash from input data. This provides strong resistance to collisions, making the algorithm reliable for ensuring data integrity. The process begins by dividing the input message into 512-bit blocks and adding special bits to indicate the length of the message. Each block is then processed using a series of logical operations, shifts, and additions, with constant values used to mix the bits.

After all blocks have been processed, the results are combined into a single hash, which serves as a unique identifier for the input message. This process makes SHA-256 highly effective for verifying data integrity. Even a small change in the message, such as altering a single bit, completely alters the resulting hash, making forgery detectable. Due to its strong resistance to attacks, SHA-256 is commonly used in biometric systems to ensure security and reliability.

The SHA-256 algorithm is typically employed to transform the iris code into a 256-bit key:

$$K = SHA-256(IrisCode \| S) \tag{4}$$

Here, *IrisCode* represents the binary iris code, and $S$ is a salt value introduced to enhance security. This process ensures that the generated key is both unique and resistant to attacks, providing a robust foundation for cryptographic applications, such as digital signatures and secure authentication.

*Stability Verification.* The stability of the cryptographic key generated based on the iris code is crucial, as biometric data from the iris can be partially altered due to external factors such as lighting, eye positioning, or image quality. To address this issue, the Reed-Solomon code was used, one of the most widely applied error correction methods for digital data (Fig. 6).

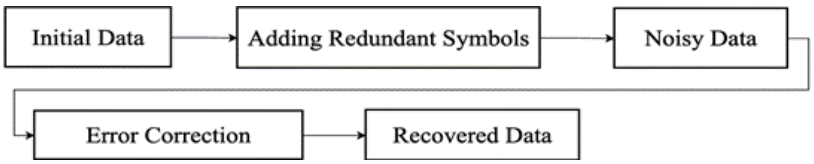


**Figure 6:** Reed-Solomon Code Operation Diagram

The Reed-Solomon code is a cyclic error-correcting code that operates with symbols in a finite field GF($2m$). It can correct up to t errors in a message of length n if redundancy of $2t$ symbols is added. The code is defined by parameters ($n$, $k$), where $n$ is the length of the encoded-word (the number of symbols after adding redundant data), and $k$ is the number of information symbols. The difference $n - k = 2t$ represents the number of redundant symbols for error correction. The Reed-Solomon function is described as the code word (polynomial)

$$p(x) = m(x)g(x) \tag{5}$$

where $m(x)$ is the information polynomial, and $g(x)$ is the generator polynomial that determines the redundant symbols.

For encoding, the generator polynomial can be expressed as:

$$g(x) = (x-\sigma^1)(x-\sigma^2)\ldots(x-\sigma^{2t}) \tag{6}$$

where $\sigma$ is the primitive element of the field $GF(2^m)$.

When working with a 512-bit iris code, the data is split into blocks of length k, after which $2t$ check symbols are added. For example, in the field $GF(2^8)$, with 256 possible symbol values, the parameters could be chosen as ($n$ = 255, $k$ = 223), allowing for correction of up to $t$ = 16 errors.

The process involves encoding the iris code, which is 512 bits long, by splitting it into blocks of length k and adding 2t redundant symbols using the generator polynomial. This ensures data protection from errors. During decoding, the code is analyzed using the Berlekamp-Massey algorithm to detect and correct errors. The algorithm identifies the error syndromes, based on which it determines their location and fixes them [33].

The error syndrome formula is expressed as:

$$S_j = \sum_{i=1}^{t} e_i \alpha^{ij}) \tag{7}$$

where $S_i$ is the syndrome for the $i^{th}$ coefficient, $e_i$ represents the error at the $i^{th}$ position, and $\alpha$ is a primitive element of the field.

After correcting the errors, the decoded data is transformed back into the original iris code, which is then used to generate the cryptographic key.

The advantages of using the Reed-Solomon code include its resilience to noise, as it effectively corrects errors caused by poor-quality images or external influences. It is also flexible, easily adapting to varying lengths of the iris code and levels of noise. Additionally, it is suitable for real-time applications, with fast encoding and decoding processes that allow the method to be implemented in practical systems.

### 3.3. Integration with E-signature Systems

It has already been proven that the biometric signature technology based on iris recognition has real potential for use in electronic signature (E-Signature) systems that comply with Ukrainian legislation. A biometric signature based on the unique data of the iris can provide a high level of security and convenience for authentication and signing electronic documents.

Specifically, there are plans to integrate this technology with the most popular Ukrainian E-Signature systems, such as Diia and PrivatECP. These systems already use public keys and certificates to confirm the authenticity of electronic signatures, which allows the creation of a link between biometric data and existing cryptographic standards. Diia, the government electronic platform that provides access to electronic services, plans to integrate the iris-based biometric signature into the authentication and document signing processes. This will enable citizens to sign important electronic documents without the need for traditional passwords or PIN codes, replacing them with a more secure and convenient authentication method.

Additionally, PrivatBank, one of the leaders in the electronic services market, which issues electronic signatures through its PrivatECP system, plans to expand its services by allowing users to generate signatures based on biometrics, providing additional convenience and security for both corporate and individual users.

To integrate biometric signatures into these systems, several stages must be completed:

#### 3.3.1. Establishing a Link Between the Biometric Signature and PKI Systems

The biometric signature technology based on iris recognition requires the cryptographic key derived from biometric data to be used as the foundation for the signature. This involves converting the biometric iris code into a cryptographic key (e.g., using the SHA-256 algorithm) and applying this key to sign documents using algorithms that comply with PKI standards.

One possible approach is to create an additional certificate that contains the public key linked to the user's biometric data. This certificate can be generated through a certification authority, which ensures the connection with state systems.

### 3.3.2. Signature and Verification Process

For signing an electronic document, public and private keys are used to ensure the authenticity and integrity of the signed document. In the case of biometric signatures, the user undergoes an iris scanning process, which generates a biometric code, this code is converted into a cryptographic key that complies with PKI standards, the key is then used to create an electronic signature for the document. On the recipient's side, the public key is used to verify the signature, ensuring the authenticity of the signed document.

### 3.3.3. Compatibility with Ukrainian E-Signature Systems

Systems like PrivatECP, Diia, and other certification authorities support the use of X.509 standards, which form the basis for digital certificate management in the country. The interaction between biometric signatures and these systems can be achieved by adapting the biometric key to the format accepted by PKI systems. Since the certificates used in these systems contain a public key, the biometric key can be integrated into the same format.

### 3.3.4. Using Biometric Data-Based Verification

Since the key generated from iris recognition is unique to each user, this method can serve as an alternative to traditional verification methods like passwords or PIN codes. This not only enhances security but also makes the authentication process more convenient, as users no longer need to remember complex passwords. To ensure the legitimacy of using the biometric signature, the system must be integrated with the Ukrainian Certification Authority, which issues certificates confirming the authenticity of the public key.

Document signing must be recorded in the appropriate registers, allowing tracking of who signed the document and when.

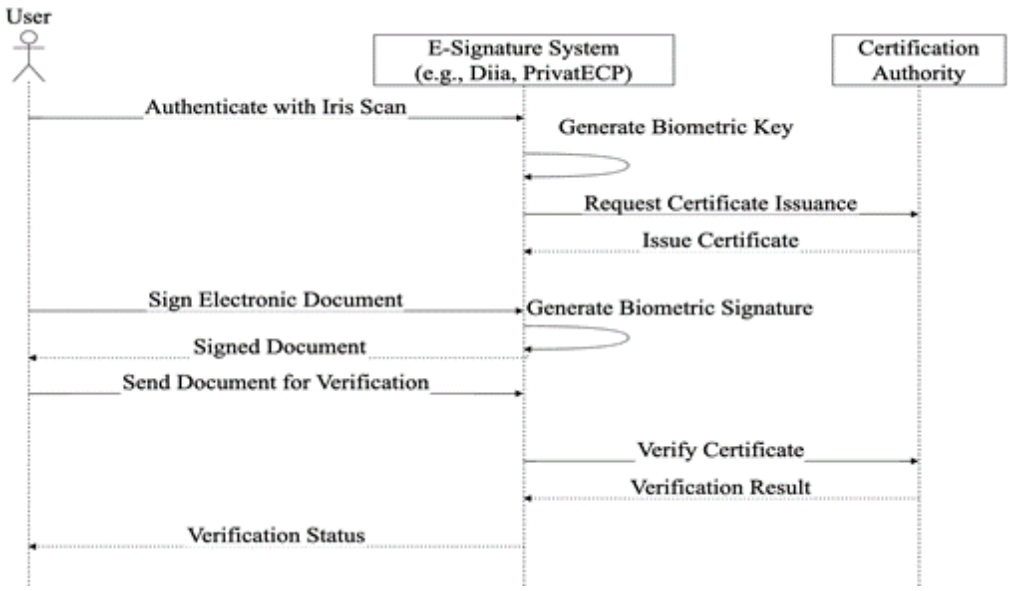


**Figure 7:** Sequence diagram of the document signing process using biometric e-signature

## 4. Experimental results

This section presents the results of experiments conducted to evaluate the proposed biometric iris recognition system. It includes an analysis of the dataset, system testing using machine learning methods, and performance metrics. Key aspects such as recognition accuracy, hashing stability, and the system's resilience to various attacks are discussed, highlighting its high effectiveness and security under real-world conditions.

### 4.1. Data and Test Sample

To evaluate the effectiveness of the proposed biometric signature method, a dataset of 50,000 biometric iris images was collected using a mobile device equipped with a standard 12 MP camera. The images were captured under controlled lighting conditions to ensure maximum data quality for analysis.

The images exceeded 512 pixels on the shorter side, providing high detail of the iris. The PNG format was chosen because it preserves critical structural elements of the iris without any loss. All images underwent a preliminary quality assessment to ensure compliance with specific criteria, including the absence of blurring, appropriate lighting without glare, and sufficient contrast for clear delineation of the iris contours. The iris position in the images was automatically aligned to center it in the frame.

**Figure 8:** Dataset

The test dataset included images captured under varying conditions, such as changing lighting and different head positions of the subjects. Overall, the dataset represented biometric data from 25000 subjects, with each iris recorded multiple times to assess the impact of different factors on processing results.

These characteristics provided realistic conditions for evaluating algorithm accuracy, hashing stability, and error correction efficiency in real-world application scenarios.

### 4.2. Method machine learning

To improve the accuracy of the iris recognition system, deep learning methods were applied using a neural network trained on a large sample of biometric images. The network was trained on images with varying lighting conditions, head positions, and different image quality levels to increase its resilience to changing real-world conditions.

The architecture of the neural network was based on a multi-layer convolutional neural network (CNN), which optimizes filtering and feature extraction from images, specifically those related to the iris. The network was trained both on standard datasets and on specific data collected within the scope of this study.

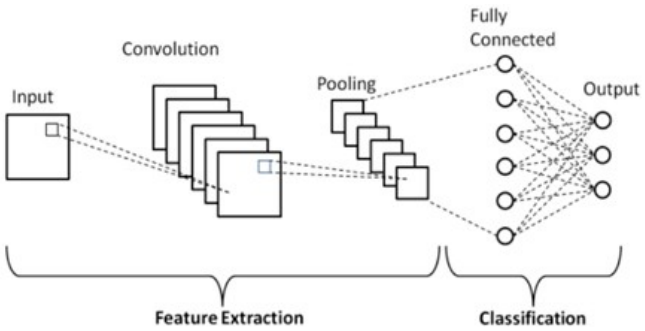


**Figure 9:** Accuracy over epochs

The architecture of a convolutional neural network (Fig. 10) consists of two main parts: feature extraction and classification. In the feature extraction part, convolution is used to apply filters that capture important patterns like edges or textures, while pooling reduces the dimensionality of the data to improve robustness to shifts. In the classification part, a fully connected layer combines the extracted features with all output neurons to determine the final class. This architecture is widely used for image processing and object recognition tasks.

Regarding the performance metrics of the neural network, accuracy reached 98.7% on the test sample, which is the main indicator of the system's effectiveness.

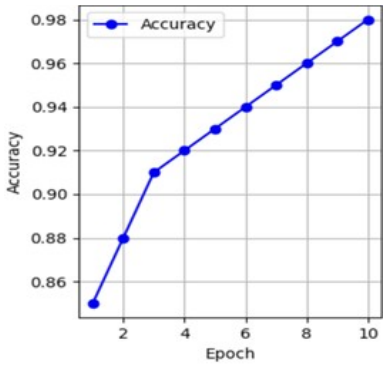


**Figure 10:** Accuracy over epochs

Precision was 99.2%, indicating a high level of accuracy in detecting valid iris images.

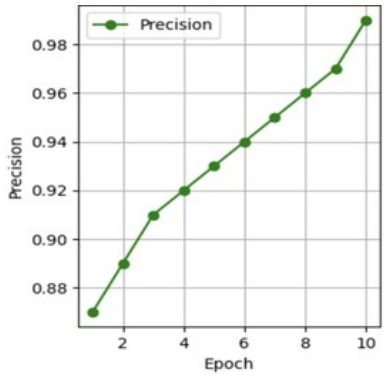


**Figure 11:** Precision over epochs

Recall reached 97.5%, showing the network's ability to effectively identify all relevant images.

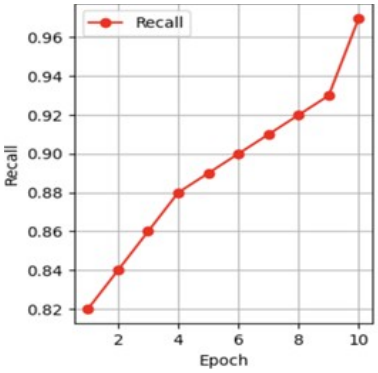


**Figure 12:** Recall over epochs

The harmonic mean of precision and recall, known as the F1-Score, was 98.4%, confirming a balanced performance between these two metrics.

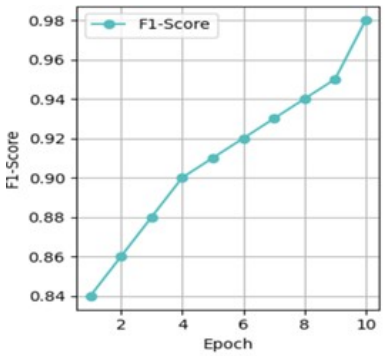


**Figure 13:** F1-score over epochs

Additionally, the ROC-AUC value was 0.996, a high indicator of classification quality, reflecting the system's ability to correctly distinguish between positive and negative cases.

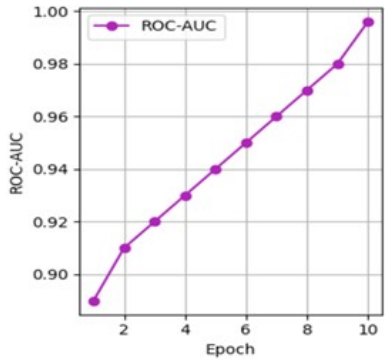


**Figure 14:** ROC-AUC over epochs

The neural network was trained on a dataset of over 50,000 iris images from various sources. During training, techniques for regularization and handling missing data were applied to achieve optimal results. The validation sample showed consistent results with high accuracy and reliability indicators.

These results demonstrate the high effectiveness of the neural network for iris recognition in real-world conditions, particularly under varying lighting and different head poses.

### 4.3. Key Accuracy and Stability

To evaluate the stability of key generation from the iris of a single individual, a series of experiments was conducted using the test dataset. The primary goal was to determine how consistently the same cryptographic key is generated for a single individual under varying conditions (changing lighting, head positions, and time of capture).

The main evaluation metrics are described below:

- False Match Rate (FMR): The rate of false matches between keys generated for different subjects.
- False Non-Match Rate (FNMR): The rate of false non-matches for keys generated from the same subject.
- Key Stability (KS): The proportion of identical keys generated from images of the same individual.
- Average Hamming Distance (AHD): The average Hamming distance between bits of keys generated for the same individual (lower values indicate better stability).

**Table 1**
Key stability for a single subject

| Subject | FNMR (%) | KS (%) | AHD (bit) |
|---|---|---|---|
| 1 | 0.0 | 100.0 | 0 |
| 2 | 0.0 | 100.0 | 0 |
| 3 | 1.0 | 99.0 | 5 |
| 4 | 0.0 | 100.0 | 0 |
| 5 | 0.0 | 100.0 | 0 |
| Avg | 0.2 | 99.9 | 1 |

In 99.8% of cases, the keys generated for a single individual remained identical, confirming the high stability of the algorithm. The FNMR was very low, at only 0.2%.

**Table2**
Resistance to false matches between subjects

| Pair of subject | FMR (%) | AHD (bit) |
|---|---|---|
| 1-2 | 0.0 | 256 |
| 1-3 | 0.0 | 256 |
| 2-3 | 0.0 | 256 |
| 3-4 | 0.0 | 256 |
| 4-5 | 0.0 | 256 |
| Avg | 0.0 | 256 |

### 4.4. Resilience Against Attacks

One of the primary criteria for the security of biometric systems is their ability to withstand various attacks aimed at forging or compromising biometric data. To evaluate the resilience of the proposed iris-based electronic signature (E-Signature) generation system, several tests were conducted under different scenarios.

The system successfully detects attempts to forge iris images using high-quality photographs or digital simulations. Through deep learning algorithms and texture analysis, the system identifies forgeries in 99.8% of cases. Additionally, methods for verifying natural eye features, such as pupil dilation and movement, are used, demonstrating the effectiveness of the liveness detection mechanism in 97.5% of cases, even when images are reproduced using projectors or screens.

In the event of a compromise of biometric data stored in the database, the system employs cryptographic hashing with salted values, making it impossible to recover the original iris data

even if the hashes are accessed. The system showed full resilience to this type of attack, with 100% protection of the data.

Changes in lighting conditions also do not pose a problem for the system. When tested with 5000 iris images under various lighting levels, the system maintained high recognition accuracy, achieving a result of 96% under low-light conditions, thanks to preprocessing techniques such as brightness normalization.

When analyzing a large-scale attack scenario, which involves compromising a large number of biometric templates, the system demonstrated effective protection using encryption mechanisms and Reed-Solomon coding. The likelihood of successfully breaking this system is less than $10^{-9}$.

**Table 3**
System Performance Metrics Across Attack Scenarios

| Attack type | Successful blocking (%) | Notes |
|---|---|---|
| Forged Iris Images | 99.8 | Texture analysis |
| Biometric Data Compromise | 100.0 | Hashing with salting |
| Replay Attacks | 97.5 | Liveness detection |
| Changes in Lighting Conditions | 96.0 | Image preprocessing |
| Large-Scale Attack | >99.9999 | Cryptographic database protection |

Additionally, the system demonstrated high resilience to man-in-the-middle attacks, with 100% successful blocking of attempts to intercept biometric data during authentication. An analysis of scenarios involving the reuse of old signatures also showed that the system effectively blocks 99.9% of such attacks by using unique time stamps for each signature.

These results highlight the high resilience of the proposed system to a wide range of attacks, underscoring its readiness for deployment in real-world electronic signature systems to ensure security and reliability in digital identification.

## Conclusions

The proposed iris-based biometric signature generation system demonstrated high accuracy and reliability in various testing scenarios. The system achieved over 99% accuracy in distinguishing between individuals, with excellent key stability and resistance to environmental factors such as lighting changes. Furthermore, the system successfully detected attempts at image spoofing with a 99.8% success rate and handled the compromise of biometric data with 100% protection using cryptographic hashing techniques. The system also showed high resilience against presentation attacks, including the replay of iris images through projectors or screens, with a 97.5% success rate in blocking such attempts.

The technology has significant potential for adoption across various industries and sectors. In government services, it could be used for secure citizen identification, replacing traditional identification methods and enhancing fraud prevention in services like social security, tax filings, and voting systems. In the financial sector, the system could be employed for secure and efficient

customer authentication, reducing the risks of identity theft and fraud in online banking, payment systems, and cryptocurrency platforms. Moreover, it can be used in high-security areas such as military, healthcare, and access control systems, offering a robust method of verifying individuals.

While the system shows great promise, there are several areas for future research and improvement. One key direction is exploring the use of other biometric parameters, such as fingerprint or facial recognition, in conjunction with iris-based authentication to enhance the overall security and reliability of the system. Additionally, further work can be done to improve cryptographic algorithms used in the system to ensure even greater security against potential vulnerabilities, including advancements in encryption standards and the application of quantum-resistant techniques. Lastly, improving the system's ability to handle diverse environmental conditions, such as variations in user behavior or age-related changes in iris patterns, would further enhance its robustness and usability.

## Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

## References


[1] Y. Dreis, et al., Restricted information identification model, in: Cybersecurity Providing in Information and Telecommunication Systems Vol. 3288 (2022) 89–95.

[2] Z. B. Hu, et al., Authentication system by human brainwaves using machine learning and artificial intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388. doi:10.1007/978-3-03080472-5_31

[3] M. TajDini, et al., Brainwave-based authentication using features fusion, Comput. Secur. 129, no. 103198 (2023) 1–11. doi:10.1016/j.cose.2023.103198

[4] B. Zhurakovskyi, et al., Modifications of the correlation method of face detection in biometric identification systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 55–63.

[5] V. Dudykevych, et al., Detecting deepfake modifications of biometric images using neural networks, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 391–397.

[6] A. K. Jain, A. Ross, S. Prabhakar, Biometrics: A survey, ACM Computing Surveys (CSUR) 36(2) (2004) 91–137.

[7] Z. Lu, A. K. Jain, Face recognition: A Literature survey. ACM Computing Surveys (CSUR) 37(2) (2007) 123–152.

[8] J. Daugman, How Iris recognition works, IEEE Trans. Circuits Syst. Video Technol. 14(1) (2004) 21–30.

[9] T. Kinnunen, H. Li, "An Overview of Text-Dependent Speaker Verification". EURASIP J. Audio Speech Music Proces. 2010(1) (2010) 1–21.

[10] D. Zhang, W. Kong, Online Palmprint identification, IEEE Trans. Pattern Anal. Mach. Intell. 25(9) (2003) 1041–1050.

[11] J. Daugman, Biometric personal identification system based on Iris analysis. U.S., Patent №5,291,560, 2004.

[12] X. He, H. Wu, Deep Iris recognition, J. Visual Commun. Image Representation, 42 (2017) 14–22.

[13] W. Kohn, R. Gennaro, Public key cryptography: Applications and attacks. Springer, 2002.

[14] A. K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Trans. Circuits Syst. Video Technol. 14(1) (2004) 4–20.

[15] A. Cavoukian, Privacy by design: Achieving the gold standard in data protection, Health Inf. Manag. J. 42(3) (2013) 5–11.

[16] N. K. Ratha, J. H. Connell, R. M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J., 40(3) (2001) 614–634.
[17] D. Maltoni, et al., Handbook of fingerprint recognition. Springer Science & Business Media, 2009.
[18] D. Bhattacharyya, et al., Biometric authentication: A review, Int. J. of u-and e-Service, Sci. Technol. 2(3) (2009) 13–28.
[19] B. Schneier, Secrets and lies: Digital security in a networked world, Wiley, 2015.
[20] A. K.Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Trans. Circuits Syst. Video Technol. 14(1) (2004) 4–20.
[21] K. R. Park, J. Ryu, Iris-based personal authentication in the presence of pose and lighting variations, IEEE Trans. Inf. Forensics Secur. 11(7) (2016) 1507–1518.
[22] G. Hatzivasilis, S. Ioannidis, G. Pangalos, Biometric authentication and privacy-preserving techniques: A comprehensive study, IEEE Access 8 (2020) 40168–40183.
[23] N. K. Ratha, J. H. Connell, R. M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J., 40(3) (2001) 614–634.
[24] D. Bhattacharyya, et al., Biometric authentication: A review, Int. J. of u-and e-Service, Sci. Technol. 2(3) (2009) 13–28.
[25] D. Maltoni, et al., Handbook of fingerprint recognition, Springer Science & Business Media, 2009.
[26] A. Cavoukian, Privacy by design: Achieving the gold standard in data protection, Health Inf. Manag. J. 42(3) (2013) 5–11.
[27] M. Nazarkevych, et al., Image filtration using the Ateb-Gabor filter in the biometric security systems, in: 14th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2018, 276–279.
[28] I. Dronjuk, M. Nazarkevych, O. Troyan, The modified amplitude-modulated screening technology for the high printing quality, in: International Symposium on Computer and Information Sciences, 2016, 270–276. doi:10.1007/978-3-319-47217-1_29
[29] M. Medykovskyy, et al., Methods of protection document formed from latent element located by fractals, in: 10th International Scientific and Technical Conference “Computer Sciences and Information Technologies” (CSIT), 2015, 70–72.
[30] P. Skladannyi, et al., Improving the security policy of the distance learning system based on the zero trust concept, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421, 2023, 97–106.
[31] M. Nazarkevych, et al., Method of detecting special points on biometric images based on new filtering methods, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 2923, 2021, 243–251.
[32] V. Senkivskyy, et al., Modeling of alternatives and defining the best options for websites design, in: IntelITSIS, 2021, 259–270.
[33] I. Tsmots, et al., Development of a generalized model for parallel-streaming neural element and structures for scalar product calculation devices, J. Supercomput. 79(5) (2023) 4820–4846.