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

BOUHISSI Houda El, YURKO Pavlo
Khmelnytskyi National University

ANALYSIS OF BIOMETRIC ACCESS CONTROL SYSTEMS

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

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

БУХІССІ Худа Ель, ЮРКО Павло
Хмельницький національний університет

АНАЛІЗ СИСТЕМ КОНТРОЛЮ ПРОПУСКУ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

У статті представлено розроблений метод та програмно-технічний засіб для організації системи контролю пропуску на основі біометричних даних. Запропонований метод включає етапи збору, попередньої обробки, зберігання та перевірки біометричних ознак, таких як відбитки пальців, зображення обличчя та сканування райдужної оболонки ока з метою ідентифікації та аутентифікації особи. Застосування біометричних характеристик дозволяє значно підвищити рівень захисту інформаційних систем, приміщень або інших ресурсів, доступ до яких має бути суворо обмежений. На відміну від традиційних систем безпеки, що базуються на використанні паролів чи ключових карток, запропоноване рішення мінімізує ризики компрометації облікових даних, передачі засобів доступу третім особам або втрати ідентифікаційних носіїв.

Описаний програмно-технічний засіб забезпечує інтеграцію спеціалізованих біометричних сенсорів, системи обробки та зберігання даних, а також алгоритмів аутентифікації та прийняття рішень у режимі реального часу. Рішення орієнтоване на масштабоване впровадження в різних галузях — від підприємств та освітніх закладів до об'єктів критичної інфраструктури. Система дозволяє ефективно керувати потоком осіб, які мають право на доступ, автоматизувати процес перевірки, забезпечити протоколювання подій, а також інтеграцію з іншими системами безпеки. Особливу увагу приділено захисту біометричних даних відповідно до сучасних вимог з інформаційної безпеки та конфіденційності. Представлений підхід спрямований на забезпечення високої надійності, зручності використання та зменшення ймовірності несанкціонованого доступу, підвищуючи загальний рівень безпеки середовища.

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

Introduction

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

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

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

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

Domain analysis

In today's digital world, electronic devices, including biometric access systems, are becoming increasingly widespread. Examples of such technologies can be seen in embedded systems used in smartphones, Global Positioning Systems (GPS) [3], and tablets. With the rapid development and extensive deployment of communication networks, millions of devices utilizing biometric data are connected to the global infrastructure.

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

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

(a) knowledge — information the user knows, such as passwords;
(b) tokens — physical items the user possesses, such as access cards or badges;
(c) biometrics — unique user characteristics, such as fingerprints, iris patterns, or movement dynamics [3].

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

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

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

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

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

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

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

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

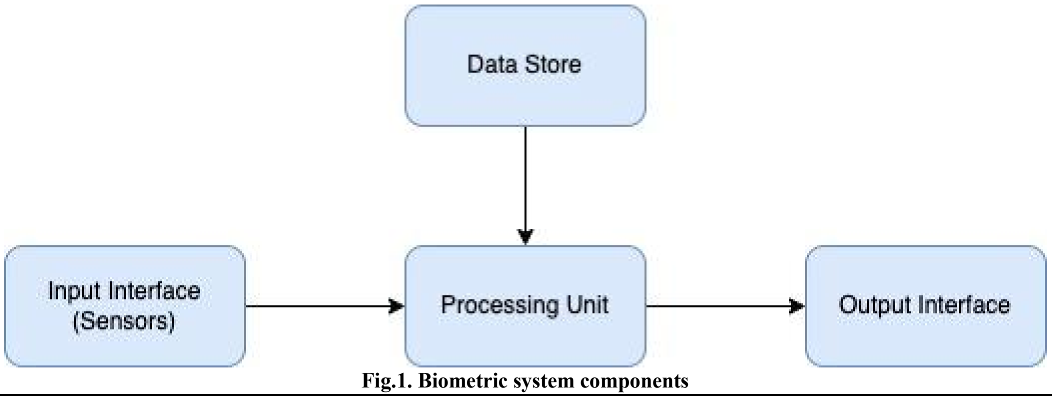

Fig.1. Biometric system components

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

The risks of the usage of biometric data are to be expected, as there is nothing perfect and there is no 100% guarantee that the data and confidentiality are completely protected and no one can hack them. Most of the risks include theft of biometric templates, misuse of the data by hackers or identity thieves, and even the possibility of falsification of the data also known as spoofing, which could be considered the most dangerous type of risk.

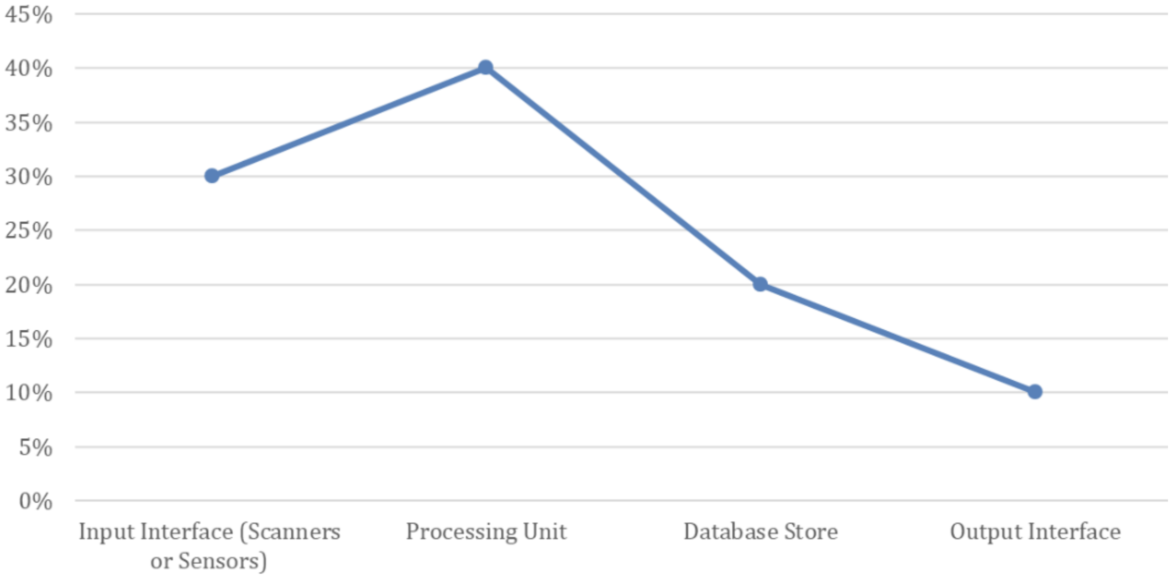

Fig 2. Distribution of Biometric System Components by Their Percentage Shares

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

Analysis of existing solutions and technologies

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

Fingerprint Recognition

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

Facial Recognition

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

Iris Recognition

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

Biometric authentication technologies offer various advantages, depending on the use case. **Fingerprint recognition** is widely used due to its affordability and reliability, though it has vulnerabilities related to spoofing and fingerprint wear. **Facial recognition** is gaining popularity for its non-intrusiveness and versatility, but privacy concerns and the potential for spoofing are significant drawbacks. **Iris recognition** offers high accuracy and robustness against spoofing but is less accessible due to high costs and less convenience.

Table 1

Comparison of Biometric Authentication Technologies

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

Definition of Similarity of Biometric Samples

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

Correlation:

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

(1)

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

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

Euclidean Distance Method:

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

(2)

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

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

Biometric Authentication:

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

(3)

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

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

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

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

False Accept Rate (FAR):

$$FAR = \frac{Number\ of\ False\ Acceptances}{Total\ Number\ of\ Rejestions} \tag{4}$$

False Reject Rate (FRR):

$$FRR = \frac{Number\ of\ False\ Rejestions}{Total\ Number\ of\ Acceptancer} \tag{5}$$

Algorithms for Improving Accuracy

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

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

Table 2.

Analysis of Main Biometric SKUDs

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

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

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

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

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

1. Face Detection.

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

2. Preprocessing.

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

3. Feature Extraction.

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

4. Face Recognition.

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

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

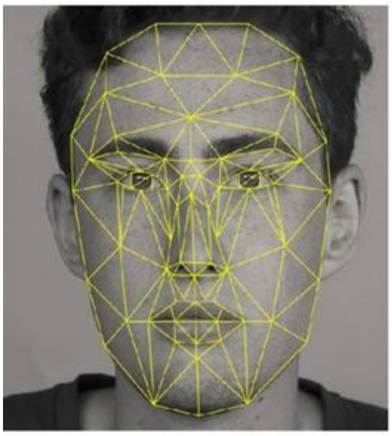

Fig. 2. Example of constructing geometric lines on a human face

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

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

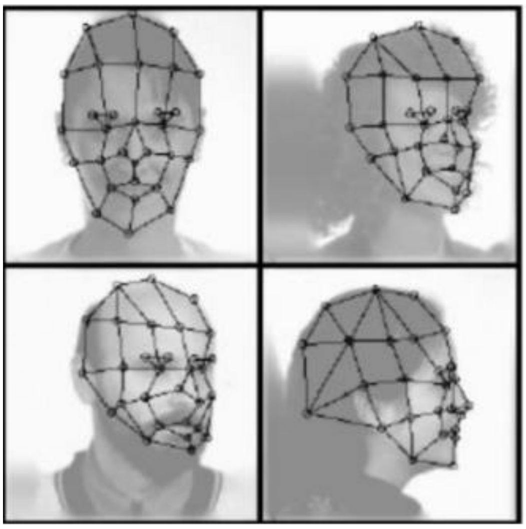

Fig. 3. Elastic Graph Matching Method

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

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

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

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

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

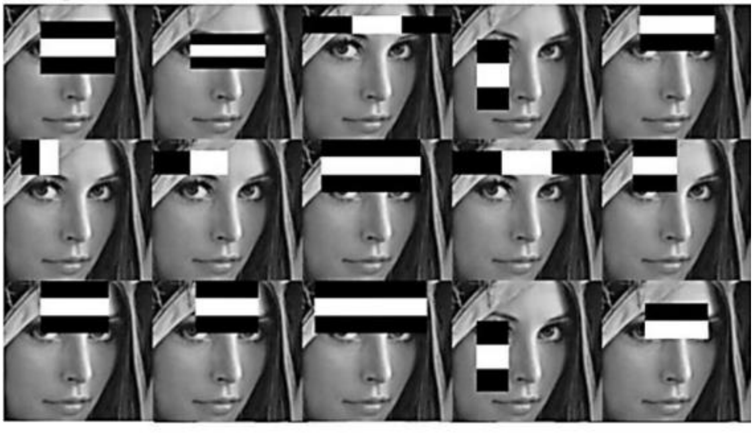

Fig. 4. Haar primitives

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

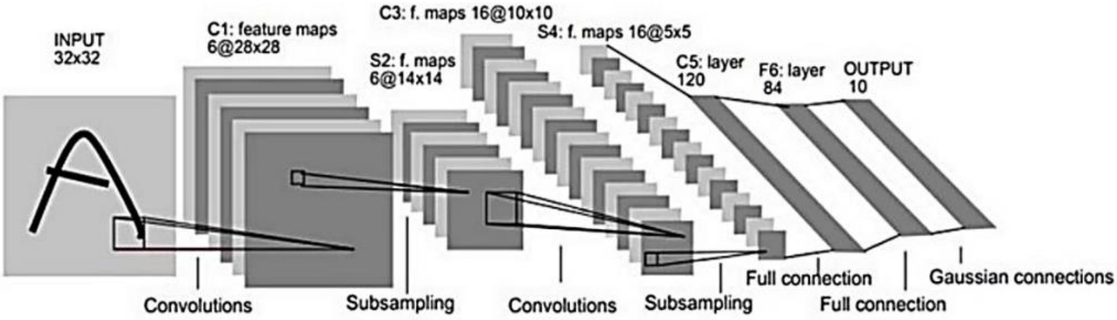

Fig. 5. Architecture of LeNet5

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

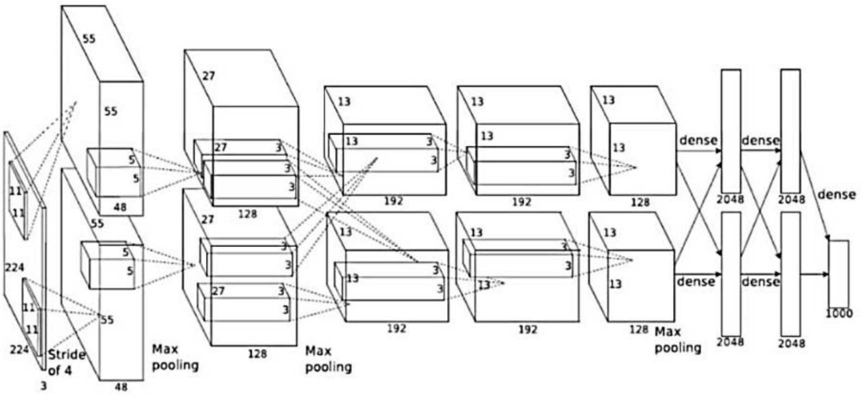

Fig. 6. Architecture of AlexNet

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

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

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

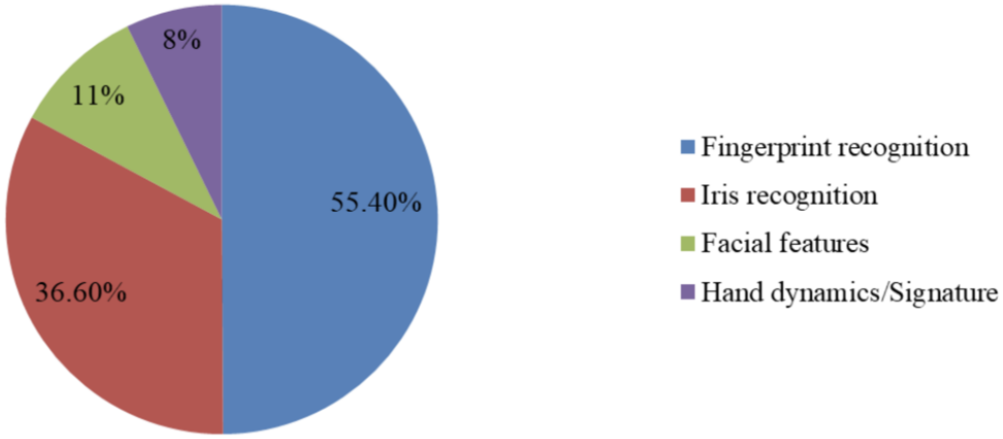

Fig.7. Distribution of Biometric Authentication Methods by Popularity

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

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

Conclusion

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

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

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

References

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

11. A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. URL: https://www.sciencedirect.com/science/article/abs/pii/S2214785321048513 (Last accessed January 27, 2025).

12. Exploring biometric identification in FinTech applications based on the modified TAM. URL: https://link.springer.com/article/10.1186/s40854-021-00260-2 (Last accessed January 27, 2025).

13. An Ensemble Approach To Face Recognition In Access Control Systems. URL: https://journals.riverpublishers.com/index.php/JMM/article/view/24241 (Last accessed January 27, 2025).

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