METHODS OF USING BIOMETRIC SYMBOLS FOR IDENTIFICATION

Shamenova Altinay
Nukus State Technical University
First-Year Master's Student in Computer Engineering

Annotation: *This article examines modern methods of using biometric symbols for human identification. Biometric identification technologies are widely used in security systems, access control, banking systems, and digital authentication. The growing need for reliable and secure identification methods has led to the development of biometric systems that rely on unique physiological and behavioral characteristics of individuals. Such characteristics include fingerprints, facial recognition, iris patterns, voice recognition, and signature dynamics.The study analyzes the main types of biometric symbols and their role in personal identification systems.Particular attention is given to the methods of collecting, processing, and analyzing biometric data in modern digital environments. The advantages and disadvantages of biometric identification technologies are also discussed, including issues related to accuracy, security, and privacy protection.Examples of the practical application of biometric identification systems in different sectors such as banking, mobile devices, and border control are presented. The results of the study show that biometric technologies significantly improve the reliability of identification systems and reduce the risks associated with traditional authentication methods such as passwords and identification cards.The article concludes that the development and implementation of biometric identification systems will continue to play an important role in improving information security and protecting personal data in the digital age.*

Keywords: *biometric identification, biometric symbols, fingerprint recognition, facial recognition, iris recognition, authentication systems, information security.*

In the modern digital era, the issue of reliable identification and authentication of individuals has become increasingly important. With the rapid development of information technologies, online services, and digital communication systems, protecting personal data and ensuring secure access to information resources has become a major challenge for organizations and governments worldwide. Traditional identification methods such as passwords, PIN codes, and identification cards are gradually becoming insufficient due to their vulnerability to theft, loss, or unauthorized access.As a result, biometric identification technologies have gained significant attention in recent years. Biometric systems are based on the analysis of unique biological or behavioral characteristics of a person, which makes them more reliable than traditional identification methods.Biometric symbols refer to measurable human characteristics that can be used to identify or verify the identity of an individual.These characteristics include fingerprints, facial features, iris patterns, voice characteristics, hand geometry, and even behavioral traits such as typing rhythm.Biometric

identification systems operate by capturing a biometric sample, extracting distinctive features, and comparing them with stored biometric templates in a database. If the similarity between the captured data and the stored template exceeds a predefined threshold, the identity of the individual is confirmed. This process makes biometric authentication highly secure and convenient for users.

In recent years, biometric technologies have been widely implemented in various sectors such as banking, healthcare, border security, and mobile technology.[1]For example, many modern smartphones use fingerprint scanners or facial recognition systems to unlock devices and authorize payments. Similarly, airports and border control systems increasingly rely on biometric identification to verify the identity of travelers and improve security measures.Despite their advantages, biometric systems also face several challenges.These include issues related to privacy protection, data storage security, and the possibility of false acceptance or rejection. Therefore, the development of effective methods for using biometric symbols for identification remains an important research area in information technology and cybersecurity.The purpose of this article is to analyze the main methods of using biometric symbols for identification and to examine their applications in modern technological systems.Biometric identification systems rely on the use of unique biological characteristics of individuals.These characteristics are commonly referred to as biometric symbols or biometric traits.They can be divided into two main categories: physiological biometrics and behavioral biometrics.

Physiological biometrics are related to the physical characteristics of a person. The most common examples include fingerprint recognition, facial recognition, iris recognition, and palm geometry.[2]Behavioral biometrics, on the other hand, are based on patterns of human behavior such as voice recognition, typing rhythm, or signature dynamics.One of the most widely used biometric identification methods is fingerprint recognition. Fingerprints consist of unique patterns of ridges and valleys on the surface of human fingers. Even identical twins have different fingerprint patterns. Fingerprint recognition systems work by scanning the fingerprint and extracting key features such as ridge endings and bifurcations.These features are then converted into a digital template and stored in a database.For example, many smartphones today use fingerprint scanners to unlock the device. When the user places their finger on the scanner, the system compares the scanned fingerprint with the stored template.If a match is found, the device is unlocked. This method is widely used because it is fast, reliable, and convenient.Another important biometric identification method is facial recognition. Facial recognition systems analyze various facial features such as the distance between the eyes, the shape of the nose, and the contour of the jawline. These features are converted into a mathematical model that represents the individual's face.Facial recognition is widely used in security systems and surveillance technologies. For example, airports use facial recognition systems to verify passengers' identities during border control procedures. Cameras capture the passenger's face and compare it with the photo stored in their passport database.

Iris recognition is considered one of the most accurate biometric identification methods.[3]The iris is the colored ring around the pupil of the eye and contains complex patterns that are unique to each individual. Iris recognition systems use high-resolution cameras to capture detailed images of the iris and analyze its unique patterns.For instance, some high-security facilities and research laboratories use iris scanners to control access to restricted areas. Because iris patterns remain stable throughout a person's life, this method provides a high level of accuracy and security.

Voice recognition is another example of behavioral biometric identification. Voice recognition systems analyze the unique characteristics of a person's speech, including pitch, tone, and pronunciation patterns. These systems are often used in telephone banking and virtual assistants.For example, some banks allow customers to access their accounts using voice authentication. The system analyzes the customer's voice and compares it with the stored voice template before granting access.Despite their advantages, biometric systems also have certain limitations. Environmental factors such as lighting conditions can affect facial recognition accuracy, while injuries or dirt on fingers may affect fingerprint recognition. Additionally, storing biometric data requires strong security measures to prevent unauthorized access.Modern biometric systems often combine multiple biometric methods to increase reliability. This approach is known as multimodal biometrics. For example, a security system may use both fingerprint and facial recognition to verify a person's identity. By combining different biometric traits, the system reduces the risk of identification errors and improves overall security.

Biometric identification technologies have become an essential component of modern security systems.[4]The increasing demand for reliable and secure authentication methods has led to the widespread adoption of biometric systems in various sectors, including banking, healthcare, border control, and mobile technologies.The analysis presented in this article shows that biometric symbols provide a highly effective means of identifying individuals based on their unique physiological and behavioral characteristics. Unlike traditional identification methods such as passwords or identification cards, biometric traits cannot easily be lost, forgotten, or stolen. This makes biometric authentication more reliable and convenient for users.Among the most commonly used biometric identification methods are fingerprint recognition, facial recognition, iris recognition, and voice authentication. Each of these methods has its own advantages and limitations.[5]

Fingerprint recognition is widely used due to its simplicity and reliability, while facial recognition systems are convenient for large-scale surveillance and access control. Iris recognition provides extremely high accuracy, making it suitable for high-security environments.However, the implementation of biometric systems also raises important concerns related to privacy protection and data security. Since biometric data represents unique personal information, it must be stored and processed using secure encryption methods to prevent unauthorized access. In addition, developers of biometric systems must address potential issues such as false acceptance and false rejection rates.The development of

multimodal biometric systems represents an important step toward improving identification accuracy and reliability. By combining multiple biometric traits, these systems significantly reduce the risk of authentication errors and increase overall security.In conclusion, biometric identification technologies will continue to play a crucial role in modern information security systems. As technology continues to advance, biometric systems are expected to become more accurate, faster, and more widely accessible. Future research should focus on improving the efficiency of biometric algorithms, enhancing privacy protection mechanisms, and developing new biometric identification methods.

References

1. Bolotov A.A. Biometric personality identification systems. - Moscow: Hotline - Telecom, 2015.
2. Ivanov A.I. Biometric Identification of Personality. - Moscow: KNORUS, 2017.
3. Malyuk A.A. Information Security: Fundamentals of Information Protection. - Moscow: Hotline - Telecom, 2016.
4. Petrenko S.A. Methods of biometric identification. - Moscow: BHV-Petersburg, 2014.
5. Khoroshko V.A. Biometric Technologies in Safety Systems. - Moscow: Radio and Communication, 2013.