31. BIOMETRIC AUTHENTICATION

Solonovich V.S.

Belarusian State University of Informatics and Radioelectronics

Minsk, Republic of Belarus

Maksimchuk R. T. - Senior Lecturer

Biometric authentication, often called biometrics, with its historical origins, key traits and its operational process is presented in this paper. The advantages of this technology are highlighted, and potential risks are emphasized.

It is not widely known that the history of biometrics dates back to the late Middle Ages, specifically to the 14th century. It was a time when Chinese merchants used fingerprints to verify the identity of their business partners. According to Chinese historians, there was a custom to put inked fingerprints to sign legal documents such as loan and debt contracts. Afterwards, in 1869, Sir Francis Galton advanced the study of fingerprints, creating a classification system that remains in use today. While the 19th and 20th centuries focused on

research and development in scientific fields, biometrics has experienced remarkable technological growth in the 21st century. Consequently, in 2013 Motorola became the first company to implement a fingerprint scanner into a smartphone [1].

Generally, biometric authentication is a technology that identifies individuals by utilizing biological data and depends on distinct physical and behavioral attributes, which are highly intricate and almost impossible to replicate. Physical characteristics include fingerprints, palm prints, eyes (retina and iris), body odor, facial skin, skin pores, deoxyribonucleic acid (DNA-genetic material), blood vessels, hand textures, etc. They are referred to as biometric modalities. Behavioral characteristics include signatures, voice, facial expressions, the gait of walking, keystroke patterns, writing style.

Turning to the operational aspect of biometric technology, it is essential to examine the stages that constitute its process. The biometric authentication procedure involves three fundamental steps.

- Enrollment. The individual's biometric data is collected, stored and subsequently examined to prevent any duplication of existing entries in the secure database. It is usually accomplished by using specialized scanners, reading devices or microphones.
- Authentication**.** When access is requested to a system or facility requiring biometric verification, the user is asked to provide their biometric data. As a result, the input is captured and the corresponding data is retrieved by the system for comparison.
- Matching**.** The newly captured data is compared to a reference template stored in the database. This template serves as a basis for verifying the individual's identity. If the biometric data matches the template, the user is granted access. If not, the authentication fails, ensuring the security of the process [2].

Nowadays biometrics is applied to virtually every sphere including access control, time and attendance tracking, mobile device security, financial transactions, healthcare, border control, law enforcement, voter registration [3].

Although biometric authentication is known for providing greater security, easy installation, timeliness, restricted access, reasonable costs and minor human errors, certain drawbacks, such as privacy issues, risks of data breaches, and instances of false positives, are acknowledged. To tackle these challenges, multimodal authentication has been developed. This method involves the combination of physical characteristics, such as fingerprints, with behavioral traits, like typing patterns, ensuring that the system becomes considerably more resistant and difficult to compromise [4].

In conclusion, despite some disadvantages, biometric technology is regarded as a significant advancement in security. Solid encryption techniques and strict access controls are recommended to enhance its reliability. As cyber threats have become increasingly sophisticated, traditional methods like passwords are getting more vulnerable to attacks today. Continuous evolution in biometrics, including the integration of artificial intelligence and liveness detection, are being introduced to strengthen protection and improve the user experience.

***References**:*

1. The history of biometrics [Electronic resource]. – Mode of access: https://clockit.io/historical-timeline-biometric-authentication. – Date of access: 15.03.2025.

2. The process of biometrics [Electronic resource]. – Mode of access: https://copperpod.medium.com/the-technology-behind-biometric-authentication-how-do-machines-recognize-you-5f1f3fbc0ea3. – Date of access: 15.03.2025.

3. The applications of biometrics [Electronic resource]. – Mode of access: https://www.aware.com/what-are-biometrics-biometric-applications/. – Date of access: 15.03.2025.

4. Biometrics. Issues and challenges [Electronic resource]. – Mode of access: https://www.intechopen.com/chapters/65920. – Date of access: 15.03.2025.