PROSPECTS OF BIOMETRICS IN INFORMATION SECURITY

Juraev Dilshodbek Makhsutali ugli
Assistants of the Department of Information Technology,
Namangan institute of engineering and technology
E-mail: dilshodbek.j.m@gmail.com

Pirnazarov Ulugbek Umataliyevich
Assistants of the Department of Information Technology,
Namangan institute of engineering and technology
E-mail: upirnazarov909@mail.com

ABSTRACT

The article discusses the issue of using biometric systems in information systems from the point of view of ensuring information security. Risks that may affect safety and ways to minimize them are highlighted.

Keywords: biometric systems, identification, authentication, biometric personal data, information security.

ПЕРСПЕКТИВЫ БИОМЕТРИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Жураев Дилшодбек Махсутали ўғли
Ассистенты кафедры информационных технологий, Наманганский инженерно-технологический институт
E-mail: dilshodbek.j.m@gmail.com

Пирназаров Улугбек Уматалиевич
Ассистенты кафедры информационных технологий, Наманганский инженерно-технологический институт
E-mail: upirnazarov909@mail.com

АННОТАЦИЯ

В статье рассматривается использование биометрических систем в информационных системах с акцентом на обеспечение информационной безопасности. Анализируются потенциальные риски, которые могут оказать влияние на безопасность данных, а также предлагаются методы их снижения.

Ключевые слова: биометрические системы, идентификация, аутентификация, биометрические персональные данные, информационная безопасность.

AXBOROT XAVFSIZLIGIDA BIOMETRIKA ISTIQBOLLARI

Pirnazarov Ulug‘bek Umatalievich
Namangan muhandislik-texnologiya instituti informatsion
texnologiyalar kafedrasi assistenti
E-mail: dilshodbek.j.m@gmail.com

Juraev Dilshodbek Maxsutali o‘g‘li
Namangan muhandislik-texnologiya instituti informatsion
texnologiyalar kafedrasi assistenti
E-mail: upirnazarov909@mail.com,

ANNOTATSIYA

Ushbu maqolada raqamli iqtisodiyot tushunchasi, O’zbekistonda raqamli iqtisodiyotni rivojlanish istiqbollari yoritilgan.

Kalit so‘zlar: raqamli iqtisodiyot, axborotlashgan jamiyat, raqamli texnologiyalar, elektron hukumat.

To control access to information systems (IS), processes of user identification and authentication play an important role, which make it possible to identify a user by identifier and verify his authenticity. And if, in the most common case, these systems are based on a combination of login and password, i.e. the user must remember this combination, then in recent years there has been an increase in the popularity of systems using human biometric data, which are always with us and cannot be forgotten or lost, which provides certain convenience for users, since there is no need to remember anything or present any identification documents personality. This article will focus on biometric systems from the point of view of the issue of information security; issues of regulation of this area by the legislation of the Russian Federation, the main threats inherent in these systems and ways to minimize them will be considered. Biometric systems and their operating principles are based on the science of biometrics and biometric data. The science of biometrics refers to methods of automated recognition of a person by unique physical and/or psi recognition) and authentication (aka verification), and these concepts, as it may seem at first glance, are far from the same thing. Biometric identification (recognition) is understood as a database in which all received samples of any characteristic of all individuals for whom access is required are stored, and when compared with each of which it is possible to determine whether the applicant is the one whose characteristic is in the database or not . Biometric authentication (verification) is the process of comparing a feature from the database with the one presented to confirm the truth and make an appropriate decision on granting access to the information system. Biometric data can be divided into three groups.

Below is a classification diagram that shows the division into these three groups and subtypes of biometric technologies that belong to these groups (Fig. 1). Below the diagram is a brief description of these technologies:

Physiological characteristics:

1) Fingerprints: the theory of their uniqueness was put forward back in 1877. These days, this feature is one of the most common and well-studied; almost every modern smartphone has a fingerprint sensor.

2) Geometry of the hand: for this feature, the profile of the hand is measured, i.e. the volume of the hand and fingers, their length, as well as the unevenness of the palm and the location of the folds of skin on the folds of the phalanges of the fingers.

3) Iris: to perform recognition, video capture from a camera is used and the area of the pupil and the iris itself are highlighted using software. Next, the resulting circular image is converted into a black-and-white rectangular iris code format (similar to a QR code).

4) Retina: the method is based on recognition of the unique pattern of blood vessels and capillaries on the retina. It is complex from a technical point of view; recognition failure may occur if the pattern changes due to illness or the head is not positioned correctly during scanning.

5) Vein pattern: non-contact recognition method, based on the ability of blood hemoglobin to absorb infrared radiation. As a result of the operation of such a sensor, an image is obtained where the vein pattern is highlighted in a darker color.

6) Face: this type of recognition technology is divided into two subtypes: 2D and 3D recognition. 2D recognition is based on flat 2D images; faces in these images can be represented using algorithms as graphs with weighted vertices and edges. Three-dimensional recognition is a 3D scanning of a face using special scanners.

Psychological characteristics:

1) Handwriting and handwritten signature analysis: apply neural network theory. Today this is one of the best technologies for recognizing graphic images. Specifically for this task, supervised neural network training is used.

2) Voice and rhythm of speech: people’s voices are very different and this is due to both physiological differences (in height, weight, gender, age, mouth size) and psychological (in volume, speed, pitch, especially breathing). Modern recognition systems take into account all these factors, break the voice recording into “voice prints” and then digitize and compare them.

3) Speed and feature of typing on the keyboard: the main distinguishing characteristics of keyboard input are the period of holding a key down and the pause time between keystrokes. This method is difficult to apply to inexperienced users, because... their keyboard style is not yet fully formed. For the average user, these characteristics may be affected by psychological state (fatigue, agitation, or external distractions).

4) Gait: each person moves his body in space uniquely, since he does not just rearrange his legs, although they can also be rearranged in different ways (for example, a person may be lame for life or rearrange his legs at different speeds), but also additionally makes various movements , one of these movements is swinging your arms with different intensities.

This makes it possible for each individual to identify gait patterns and recognize a person on their basis. At this point in time, only one recognition method can be attributed to biochemical characteristics - DNA (also known as genetic fingerprinting). Any human biomaterial contains DNA, and by its distinctive features revealed during analysis, an individual can be unambiguously identified.

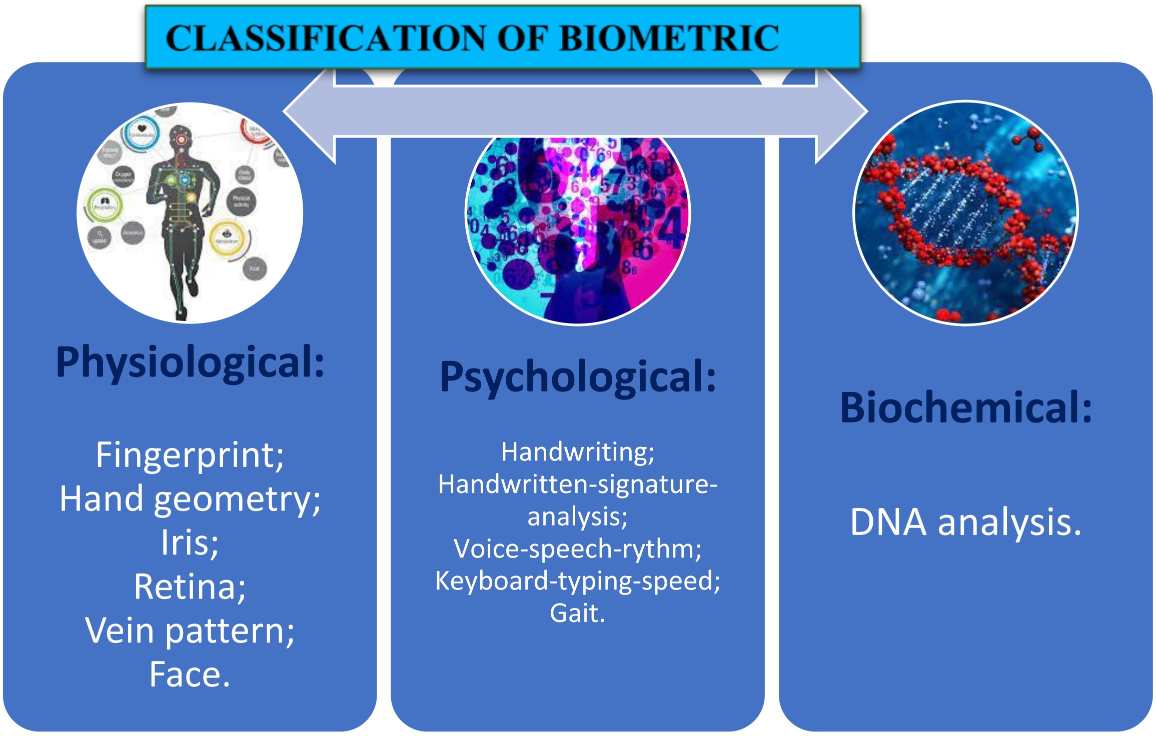

Fig. 1. Classification of biometric recognition tools

The use of artificial intelligence (AI) for biometric recognition has numerous prospects and benefits across various industries. Here are some of the key perspectives:

1. Increased security:

• Accuracy: AI algorithms can improve the accuracy of biometric recognition systems, reducing the likelihood of false positives or false negatives.

• Multimodal Biometrics: AI allows integration of multiple biometric methods (e.g. fingerprint, facial recognition, voice recognition) for stronger and more secure authentication.

2. Improved user interface:

• Convenience. AI-powered biometric recognition provides a seamless and seamless user experience, eliminating the need for passwords or traditional identification methods.

• Speed: AI algorithms can process biometric data quickly, allowing for fast authentication and access.

3. Fraud Prevention:

• Anti-spoofing techniques: Artificial intelligence can be used to implement advanced anti-spoofing techniques to detect and prevent fraudulent attempts to bypass biometric security systems using fake fingerprints, masks, or other means.

• Continuous Authentication: AI provides continuous monitoring of biometric features throughout user interactions, providing an additional layer of security against identity theft.

4. Wide range of applications:

• Mobile devices: AI-based biometric recognition is increasingly used in smartphones and other mobile devices for unlocking, payments and secure access.

• Financial transactions: AI improves the security of financial transactions through the use of biometric authentication methods, reducing the risk of unauthorized access.

5.Healthcare and medical application:

• Patient identification. AI can improve patient identification in healthcare settings using biometrics, providing accurate and secure access to medical records.

• Monitoring and alerts. AI-powered biometric monitoring can be used to detect anomalous patterns or unauthorized access to medical devices.

6. Customization and adaptability:

• Adaptation of machine learning. AI systems can adapt and improve over time through machine learning, allowing for continuous improvements in the accuracy of biometric recognition.

• User Profiles: AI can create and continually update user profiles based on changing biometric characteristics.

7. Legal and judicial applications:

• Identification of criminals. AI-based biometric recognition is essential in forensic applications to identify criminals, helping law enforcement agencies solve cases more effectively.

• Surveillance: AI can analyze large volumes of biometric data in real time from surveillance systems, helping to identify and track people.

8. Privacy Issues:

• Encryption and security: AI can be used to implement strong encryption techniques and privacy protection measures to solve problems associated with the storage and use of biometric data.

While the outlook is promising, it is critical to consider ethical considerations, privacy concerns, and potential biases in AI algorithms to ensure responsible and secure deployment of biometric recognition systems. In addition, a regulatory framework should be created to regulate the use of AI in the processing of sensitive biometric data.

Every year, the popularity of recognition technologies is growing both in the Russian and foreign markets, and due to the fact that there are no absolutely invulnerable technologies, this area is in the interests of information security specialists. According to research by J'son & Partners Consulting, based on a survey of 15 key vendors and 26 interviews with large customers, by 2020 the global biometric recognition market is projected to grow to $40 billion [2] (Fig. 2). Already, almost all new models of business-class smartphones and laptops are equipped with biometric sensors. For example, in Apple products for the mass market these are TouchID and FaceID technologies, in Microsoft it is WindowsHello. If we talk about more serious industries such as banks and business systems, then biometrics is beginning to be successfully implemented there too. For example, starting in the summer of 2018, the Unified Biometric System (hereinafter referred to as EBS), operated by Rostelecom and which is already used by some large banks in the world [2]. As already said, there are no systems that could not be completely invulnerable. One of the vectors of protection against information security violations may be compliance with information security legislation in this area. The first thing you should understand is that the biometric characteristics of all three groups relate to personal data.

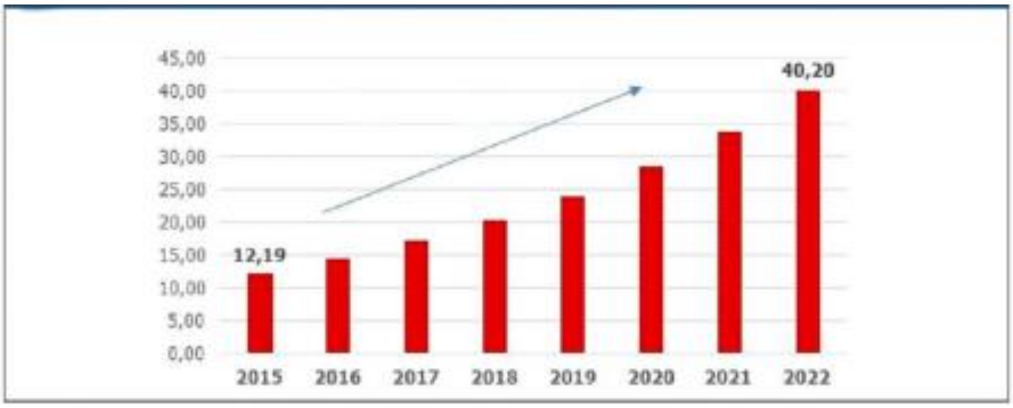

Fig. 2. Biometric technology market growth forecast

The following probabilistic concepts are associated with the reliability of sensors:
1. Errors of the first type (FRR - False Rejection Rate) - the probability of a false refusal

to the user for which access must be granted. 2. Errors of the second type (FAR - False Acceptance Rate) - the probability of erroneously granting access to an attacker. The ratio of these probabilities shows the effectiveness of the recognition system. Modern sensors and systems have low error rates and high recognition speed.

REFERENCES:

1. Methodological recommendations for banks to neutralize security threats that are relevant during the processing, including collection and storage, of biometric personal data, their verification and transmission of information on the degree of their compliance with the provided biometric personal data of a citizen of the Russian Federation. - Electron. text data – Access mode: http://www.cbr.ru/content/document/file/62907/4mr.pdf (access date: 11/07/2019). - Cap. from the screen.
2. Global market for biometric systems, 2015–2022. - Electron. text data – Access mode: http://json.tv/ict_telecom_analytics_view/ mirovoy-rynok-biometricheskih-sistem-2015-2022-gg20170119025618 (access date: 10/23/2019). - Cap. from the screen.
3. Training a neural network with a teacher, without a teacher, with reinforcement - what is the difference? Which algorithm is better? - Electron. text data – Access mode: https://neurohive.io/ru/osnovy-datascience/obuchenie-s-uchitelem-bez-uchitelja-s
4. The Central Bank decided to oblige banks to provide services using customer biometrics. - Electron. text data – Access mode: https:// www.interfax.ru/business/662298 (access date: 11/07/2019). - Cap. from the screen.
5. Experts have found a way to bypass biometric authentication by vessels. - Electron. text data – Access mode: https:// www.securitylab.ru/news/497290.php (access date: 10/23/2019). - Cap. from the screen.
6. Major Breach Found in Biometrics System Used by Banks, UK Police and Defense Firms. – Electronic text data. – Mode of access: https:// www.theguardian.com/technology/2019/aug/14/majorbreach-found-in-biometrics-system-used-by-banks-ukpolice-and-defence-firms (accessed 23 October 2019).
7. The 2017 IARPA Face Recognition Prize Challenge (FRPC). – Electronic text data. – Mode of access: https://www.nist.gov/sites/default/files/ documents/ 2017/11/22/nistir_8197.pdf (accessed October 23, 2019).
8. GOST R ISO/IEC 19784-1-2007. - Electron. text data – Access mode: http://docs.cntd.ru/document/gost-r-iso-mek-19784-1-2007 (access date: 11/07/2019). - Cap. from the screen.
9. GOST R ISO/IEC 19795-1-2007. - Electron. text data – Access mode: http://docs.cntd.ru/document/1200067413 (access date: 11/07/2019). - Cap. from the screen.
10. GOST ISO/IEC 2382-37-2016 Information technology (IT). Dictionary. Part 37. Biometrics. - Electron. text data – Access mode: http://docs.cntd.ru/document/1200144206 (access date: 10/23/2019). - Cap. from the screen.