

THE ROLE OF BIOMETRIC INFORMATION SYSTEMS IN ENSURING INFORMATION SECURITY IN INFORMATION SYSTEMS.

Saidov Jasur Doniyor o'g'li

Teacher of Gulistan State University,

Xudoyberdiyeva Muxlisa G'ulomjon qizi

Student of Gulistan State University

Abstract: This article examines the research conducted by scholars on biometric security authentication and the implementation of background checks and summarizes the analysis. Opinions on the problems encountered in the field and their solutions are given.

Key words: Biometrics, Biometric systems, FRR, FAR, EER.

Biometric systems are access control systems based on identification and authentication of a person based on biological characteristics such as DNA structure, iris pattern, retina, face geometry and temperature map, fingerprint, palm geometry. Also, these methods of authenticating a person are called statistical methods, because they exist from birth to death of a person, are with him throughout his life and can be lost or stolen. based on non-physiological characteristics. Unique dynamic biometric authentication methods are often used - signature, keyboard handwriting, voice and walking, which are based on the behavioral characteristics of people.

The concept of "biometrics" appeared at the end of the 19th century. The development of pattern recognition technologies based on various biometric characteristics has been considered for a long time, the beginning was put in the 60s of the last century. Important successes in the development of theoretical foundations of these technologies were achieved by our compatriots. However, practical results have been obtained mainly in the west and recently. At the end of the twentieth century, interest in biometrics increased significantly as the power of modern computers and improved algorithms made it possible to create a wide range of usable and interesting products in terms of their characteristics and proportions. number of users. The field of science has found its application in the

development of new security technologies. For example, a biometric system can control data access and storage in banks, it can be used in enterprises that process valuable data, to protect computers, communication devices, etc.

Description of work of biometric systems. All biometric systems work the same. First, the registration process takes place, as a result of which the system remembers the pattern of biometric characteristics. Some biometric systems take multiple samples to obtain more detailed biometric characteristics. The received data is processed and converted into a mathematical code. Biometric information security systems use biometric methods to identify and authenticate users. Biometric identification is carried out in four stages.

Registration of an identifier - information about a physiological or behavioral characteristic is converted into a form open to computer technology and entered into the memory of the biometric system. Extraction - unique features analyzed by the system are selected from the newly provided identifier. Comparison - information about the newly provided and previously registered ID is compared. Decision - A conclusion is made as to whether the newly provided identifier is a match or not.

The conclusion that the identifiers do not match can then be transmitted to other systems, which then act on the information received. One of the most important features of information security systems based on biometric technologies is high reliability, that is, the system can reliably distinguish and reliably match biometric characteristics of different people. In biometrics, these parameters are called Type I errors (False Reject Rate, FRR) and Type II Errors (False Accept Rate, FAR). The first number describes the probability of denying access to a person who has the right to access, and the second - the probability of incorrect matching of biometric characteristics of two people. It is very difficult to fake the papillary pattern of a human finger or the iris of an eye. Thus, it is almost impossible for "errors of the second kind" (that is, giving permission to someone who is not authorized to do so) to occur. However, under the influence of some factors, the biological characteristics of human identification can change. For

example, a person may catch a cold, as a result of which his voice changes beyond recognition. Therefore, the frequency of "type 1 errors" (denying access to a person who has the right to do so) in biometric systems is much higher. The better the system, the lower the FRR value for the same FAR values. Sometimes the comparative characteristic EER (Equal Error Rate) is also used, which determines the intersection point of the FRR and FAR graphs. But it is not always representative. When using biometric systems, especially facial recognition systems, even when the correct biometric features are implemented, the authentication decision is not always correct. This is due to the fact that a number of characteristics and, first of all, many biometric characteristics can be changed. There is a certain degree of probability of system error. In addition, when using different technologies, the error can vary significantly. When using biometric technologies, it is necessary to determine what is more important for access control systems, not to miss the "stranger" or not to miss all the "friends".

Types of Biometric Information Systems:

1. Biometrics Based on Physical Characteristics:

Fingerprints: Each person's fingerprints are unique and can be scanned using scanners.

Face detection: Authentication is done by detecting facial structure and geometric features.

Eye Scans: Identification by scanning the iris or retina of the eye.

Hand geometry: Identification based on the dimensions and shape of the hand.

2. Behavioral Biometrics:

Voice recognition: Authentication through human voice.

Pen or keyboard typing: Authentication through the user's typing behavior.

Gait: Identification through the way a person walks.

Advantages of Biometric Systems.

High level of reliability: Biometric features are unique and not easily forged, which ensures highly reliable authentication.

Convenience and speed: Biometric authentication for users is convenient and faster compared to traditional passwords or tokens.

Unique identification: Since the biometric characteristics of each user are unique, the probability of error in identifying them is very low.

Long-term use: Biometric features, such as your fingerprint or iris, do not change over time, which ensures long-term use.

References

1. Saidov, D., Yo'ldosheva, S., & Sayfullayeva, N. (2024). ALGORITM MURAKKABLIGI TAHLILI. *Центральноазиатский журнал междисциплинарных исследований и исследований в области управления, 1(5)*, 26-30.
2. Jasur Doniyor, O. G., Saidov, L., Allayorov, S. P., OMBORINI, S. X. I. M. L., & BAHOLASH, Y. B. Y. K. K. MEZONLARI//Scientific progress. 2021. № 1. URL: <https://cyberleninka.ru/article/n/ma-lumotlar-omborini-yaratish-bo-yicha-kasbiy-kompetentligini-baholash-mezonlari> (дата обращения: 02.06.2022).
3. Saidov, J., Abdusalolova, M., Ochilboyeva, M., & Murodova, G. (2024). MATEMATIKA, IJTIMOIIY VA TABIIY FANLAR SOHALARIGA OID ALGORITMLAR. *Theoretical aspects in the formation of pedagogical sciences, 3(7)*, 67-71.
4. Lubis, S. N., Menglikulov, B., Shichiyakh, R., Farrux, Q., Khakimboy Ugli, B. O., Karimbaevna, T. M., ... & Jasur, S. (2024). Temporal and spatial dynamics of bovine spongiform encephalopathy prevalence in Akmola Province, Kazakhstan: Implications for disease management and control. *Caspian Journal of Environmental Sciences, 22(2)*, 431-442.
5. Doniyor o'g'li, S. J. (2023). O 'ZBEKISTONDA TA'LIM TIZIMIDA BO 'LAJAK MUTAXASSISLARINING MA'LUMOTLAR BAZASI BO 'YICHA BILIMLARINI SHAKILLANTRISH. *BARQARORLIK VA YETAKCHI TADQIQOTLAR ONLAYN ILMIY JURNALI, 3(3)*, 72-77.

6. Doniyor o'g'li, S. J. (2022). PROBLEMS AND SOLUTIONS TO INCREASE THE EFFICIENCY OF DATABASE TEACHING. *European Journal of Research and Reflection in Educational Sciences*, 10(2).
7. Saidov, J., Ishchanova, I., Temirxolova, B., & Nurmammedova, Z. (2024). BILIMLAR BAZASINING ASOSIY XUSUSIYATLARI VA ULARGA OID LOYIHALASH. *Theoretical aspects in the formation of pedagogical sciences*, 3(7), 23-27.
8. Kornilov, G. P., Abdulvelev, I. R., Logunova, O. S., Kalandarov, P. I., Tursunov, O., Kodirov, D., & Abdurakhimov, D. (2022, December). Electric power supply of steel producing companies: Schematic design solutions to improve reliability of power grids. In *AIP Conference Proceedings* (Vol. 2686, No. 1). AIP Publishing.