BIOMETRIC AUTHENTICATION: MODERN METHODS OF ENSURING INFORMATION SECURITY

Saidaminxoja Abdazimov
Teacher at the Digital Technologies and Information Security of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan
Dzhamatov Mustafa
Teacher at the Digital Technologies and Information Security of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract: *In this article, we will explain how important and important biometric authentication methods are, that is, measures to use these methods in which parts of our society and in all important enterprises and organizations, as well as the "Fingerprint identification of a person" is currently the most common method and is widely used in biometric systems of information protection. It is no news to anyone that this method was widely used in the past centuries. Currently, there are three main fingerprint identification technologies. The first of them is the use of well-known optical scanners. The principle of using this device is the same as using a regular scanner. Here the main work is done by the internal light source, several prisms and lenses. The advantage of using optical scanners is their low cost. However, there are many disadvantages. These devices are quick to fail. Therefore, the user is required to use with caution. Dust, various stripes on this device will cause an error in identification, that is, it will prevent the user from logging into the system. In addition, the fingerprint captured by the optical scanner depends on the condition of the user's skin. That is, the oiliness or dryness of the user's skin interferes with identification.theoretical basis of biometric authentication, biometric The analysis of the algorithms and principles of operation of authentication methods consists of a detailed study.*

Keywords: *information Security, password, biometric technologies, Fingerprint identification, Identification by geometric dimensions of the face, Identification through the arc of the eye and the eye, identification and authentication..*

INTRODUCTION

Nowadays, computer and communication technologies are developing rapidly day by day. Because of this, it is not wrong to say that there is not a field that has not been penetrated by computer technology. The application of these modern technologies is especially effective in education, banking, and financial systems. At the same time, it is no secret that the threat to information security is growing. Therefore, one of the most urgent problems of the current era is to ensure information security.

Until now, the most widespread method of checking unauthorized access to the system is the principle of putting a “password”. Because this method is very simple,

convenient to go and requires low cost. However, by now the "password" system cannot fully justify itself. That is, a number of harms of this method became noticeable.

First, most users use simple and easy-to-remember passwords. For example, the user sets a password based on his personal dates and names. Breaking such passwords does not cause much difficulty for a voluntary person who is familiar with the user.

Secondly, during the process of entering the password, it is possible to track the characters being entered.

Thirdly, if the user uses complex, long characters when setting a password, it is possible that he himself will forget this password.

Nowadays, the existence of optional password cracking programs has become prominent. Based on the above shortcomings, it can be said that using the password principle of information protection is not fully effective. For this reason, the use of biometric methods to limit the unauthorized use of information is becoming popular around the world, and this direction is called biometrics.

Biometrics is a verification of similarity (identification) based on immutable biological characteristics of a person. Currently, biometric systems are the most reliable means of protection and are effectively used in various secret objects and in the protection of important commercial information.

Currently, biometric technologies are based on the following immutable biological characteristics of a person:

1. Through fingerprint;
2. Through the geometric dimensions of the face;
3. Through the arc of the eye and the retina;
4. By voice;

Biometric authentication of users Biometric authentication methods are chosen depending on the level of confidentiality of the organization in terms of security and how economically it can be satisfied. Biometric authentication methods are considered high-level in terms of security, so their popularization at the state level will help to contain both internal and external influences. When using biometric authentication methods in institutions, the results of user marks are performed only with “YES” or “NO” results. Based on the “YES” result, the user can enter the institution, if there will be a change in his/her signs or if there is another person, it can be known that the “NO” result or the biometric door will not open.

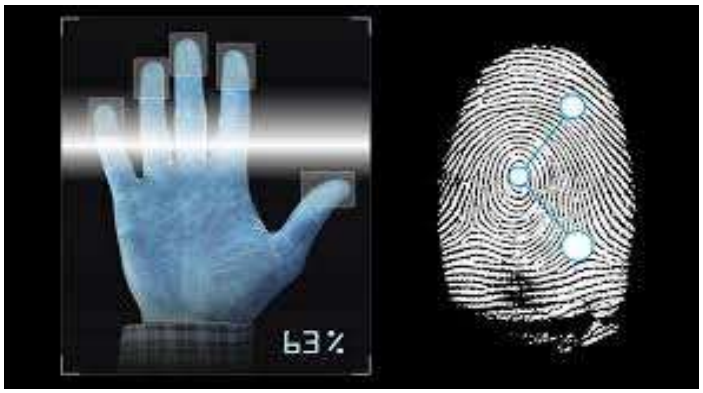
Fingerprint authentication.

“Fingerprint identification of a person” is currently the most common method and is widely used in biometric systems of information protection. It is no news to anyone that this method was widely used in the past centuries. Currently, there are three main fingerprint identification technologies. The first of them is the use of well-known optical scanners. The principle of using this device is the same as using a regular scanner. Here the main work is done by the internal light source, several prisms and lenses. The advantage of using optical scanners is their low cost. However,

there are many disadvantages. These devices are quick to fail. Therefore, the user is required to use with caution. Dust, various stripes on this device will cause an error in identification, that is, it will prevent the user from logging into the system. In addition, the fingerprint captured by the optical scanner depends on the condition of the user's skin. That is, the oiliness or dryness of the user's skin interferes with identification.

The second fingerprint identification technology is the use of electronic scanners. To use this device, the user puts his finger on a special plate made of 90,000 capacitor plates covered with silicon. In this case, a special capacitor is formed.

Among the biometric authentication systems, the most common and widespread is fingerprint identification and authentication. This system is said to be the “Dactyloscopic” method of biometric authentication.



1 Figure. Fingerprint scanning.

Today there are 3 types of fingerprinting technologies, they are as follows:

- Using ultrasounds;

-Using optical beams (FTIR);

- Using a semiconductor;

Fingerprint scanners. Traditional devices that scan fingerprints use a small optical camera that records a characteristic picture of the finger as the main element.

2 Figure. Fingerprint scanning hardware device.

Among the hardware devices of the biometric authentication system, the most reliable and popular one is the biometric authentication hardware device of the "BIOLINK" company.

Most of the manufacturers of dactyloscope devices used for scanning fingerprints mainly use integrated circuits. Such Technology companies use different types of electrical, electromagnetic and other methods to obtain fingerprints. The main reason for this is that the capacitive resistance of the skin parts is taken and analyzed during fingerprinting. During the analysis, the dactyloscopic device collects all the information in order to determine the capacitive resistance through a semiconductor sensor.

Facial structure authentication systems.

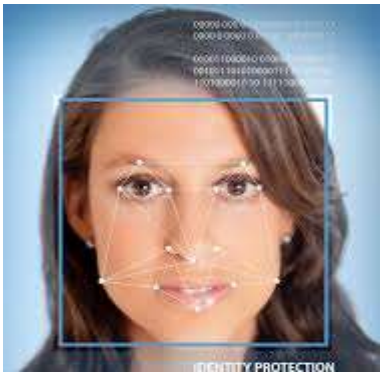
Face authentication differs in that it is universal, that is, cheap, and since all computers have a video feature, this system can be used everywhere. This system is mainly used during remote identification. The dimensions of the face are calculated on the basis of the points below (Fig. 3). These points change due to the fatness of the face. However, even when the face is fat and thin, its structure, geometric dimensions and angles do not change. Therefore, this system is considered one of the most reliable. Here, its following points are measured:

-The structure of the lip is its angle;

-Nose tip and dimensions;

- The center of the eye and the corner of the eye;

In this case, its dimensions are compared with the dimensions of the persons in the database, which shows that it is actually a person working in the institution or not. But there are enough factors that can destroy this system: glasses, beard, facial decorations, etc.



3 Figure. Authentication by facial structure.

In the case of the picture, the dimensions of the eyes, nose and lips are taken and identified. Manufacturers of facial recognition devices use proprietary mathematical algorithms to identify the user.

Eye authentication.

The Eye authentication method is mainly performed in two different ways.

1. Arc of the eye;

2. Location of Eye blood vessels;

Eye arc authentication is mainly authenticated by the radius of the eye arc and its dimensions. The image below shows the method of authentication by taking the dimensions of the radius of the eye arc and its position.

5 Figure. Retina authentication.

This biometric authentication method is considered the highest level of security. Therefore, this method of biometric authentication is placed in the offices where it is necessary to ensure a high level of security of the states.

6 Figure. Eye biometric authentication hardware device.

Eye authentication hardware device developed by Biolink. he location of the vessels in the retina has been found to be very different even in twins. But since the circle of the eye is similar to each other in some individuals, the eyelid is often used.

Voice authentication systems.

These systems can be implemented on the basis of computers with all multimedia. Therefore, these biometric systems differ from other biometric systems due to their low cost. A microphone is enough to use this system. This system works based on the frequency of a person's voice.

7 Figure. Voice authentication.

This biometric authentication method is mainly used in modern business centers and at the same time this technology is developing rapidly. There are many ways to build a template with sound. Usually, this method has frequency and its different structures and voice statistical characteristics. Therefore, its problem is that one person's voice may vary depending on the variety: vocal health, age, mood, etc. This diversity creates serious difficulties in distinguishing the unique characteristics of the

human voice. In addition, noise is another important and unsolved problem during the practical use of voice authentication.

Integral representation of images is the matching of size with the image entering the matrix. Each element (left, right and above) stores the sum of intensive pixels.

Matrix elements are calculated by the following formula:

$L(x,y)=\sum_{i=0,j=0}^{i\le x,j\le y} [\![I(i,j)]\!]$ (11)

I(i,j) - the brightness of the pixels of the incoming image.

Each L[x,y] matrix element represents a sum of pixels at right angles from [0,0] to [x,y]. Each [x,y] pixel symbol is equal to the sum of the pixel symbols to the left and above. Matrix computation is linear in time, so it computes the pixels in the image in one pass. The calculation of matrices is carried out by the following formula:

$L(x,y) = I(x,y) - L(x-1,y-1) + L(x,y-1) + L(x-1,y)$

This integral matrix can calculate the right angles and areas of the image very quickly. The representation of rectangles in the standard Viola-Jone method is called Haara reception.

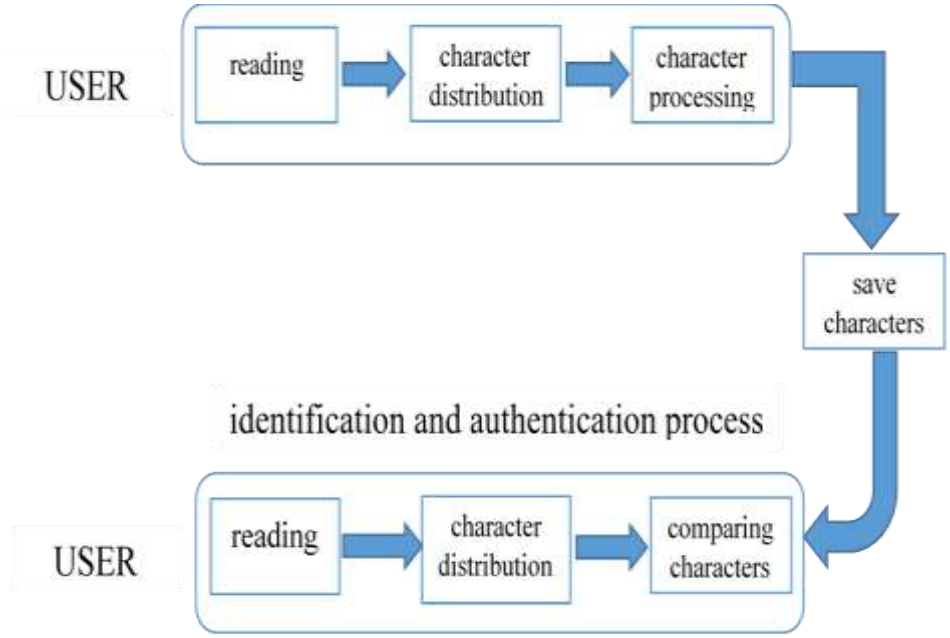
The counting of these characters is done as follows:

F = X-Y

X - is the sum of light expression in each symbol;

Y - is the total representation of darkness in each character.

The principle of operation of biometric authentication methods.



Currently, the latest standard is developed by the US NIST Institute, PVTE-12, i.e., the standard for finger scanning and its evaluation. When registering in the system, the user is required to demonstrate his characteristic symptoms one or more times. Consumer point of view in terms of the biometric authentication system is characterized by the following two parameters:

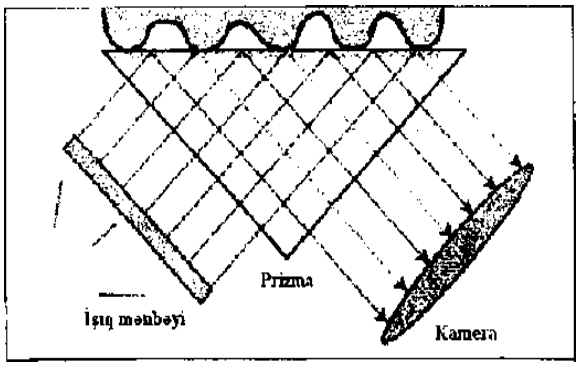
- false rejection rate FRR (false rejection rate);
- false positive rate FAR (false-alarm rate).

Fingerprint authentication uses the Recognition method. Basically, when you put your finger on the sensor, the system evaluates the fingerprint and analyzes the characteristic points of the finger. For this reason, the most common comparison algorithm is used in the fingerprint authentication method. But depending on whether the finger is dry or wet, the results may vary.

The distinguishing features of fingerprints are the main core and delta points. For example, the left ring trace has one core near the center and one delta on the right. These rings are important when using automated fingerprint dactyloscopy. The data obtained from this dactyloscope is stored in digital form.

Fingerprint scanners can be obtained in the following order:

• optical;
• silicon,
• ultrasound.

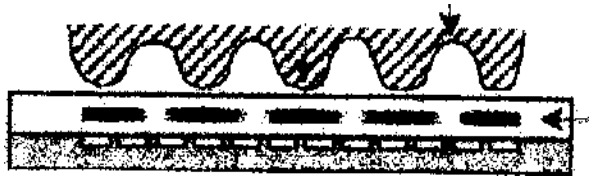


8 Figure. Optical scanner.

Currently, the following methods of optical scanning are available:

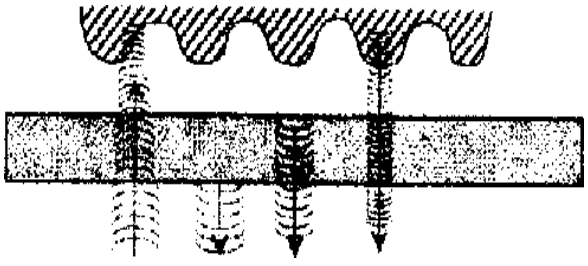
-FTIR scanner - Frustrated Total Internal Reflection (FTIR).

- Optical scanner - Fiber optic scanners. This method mainly uses matrix operations. Electro-optical scanner - Electro-optical scanners are based on this technology, electro-optical polymer is used.



9 Figure. Electro-optical sensor.

-Ultrasound scanners - information is obtained on the basis of ultrasound scanning between the level of the finger and the scanners.



10 Figure. Ultrasound scanner.

Fingerprints are presented on the inner and outer skin of a finger, and Veridicom's dactyloscopic device collects information by detecting capacitance using a semiconductor sensor. The principle of sensor operation is as follows: The finger placed on this scanner acts as one of the condenser plates. The second capacitor located on the surface of the sensor consists of 90,000 sensitive plate silicon miroschema. The small size and low price of fingerprint sensors based on integrated circuits make them an ideal interface for a security system. They can be mounted on key fobs. As a result, the user will have a universal key that ensures secure use of doors from the computer to the entrance, cars and ATMs.

CONCLUSION

As we ensure information security with the help of biometric methods, the first question that is asked to us is which biometric method, at what price and for how many people we can install it in an enterprise, organization or institution. In addition, the level of security and economy of the enterprise helps to choose biometric methods. Each enterprise, organization or institution organizes a security system based on its economic aspect. In situations where the security system does not need to be high, the biometric authentication method using face and voice will satisfy this enterprise, organization or institution.

If an enterprise, organization or institution has high security requirements and satisfies all biometric authentication methods from an economical point of view, in such a situation, the biometric authentication method using the arc of the eye and the retina is the best method. But if there is a situation where the economic price is not high and the number of workers is large, in such a situation, the method of biometric authentication with the help of a finger can provide a sufficient level of security in this enterprise.

REFERENCES:

1. Ganiev S. K.,Karimov M. M. “Information protection in computing systems and networks”: Study guide for students of higher educational institutions.

2. A.B.J.Teoh, A.Goh, and D.C.L. Ngo, "Random Multispace Quantizion as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs”, Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 28, pp. 1892—1901, 2006.

5. Magnuson, S (January 2009), "Defense department under pressure to share biometric data", National Defense Magazine.org.

6. www.security.uz/node/277734.

7. www.google.co.uz/digest/9735.htm

8. www.itv.ru/products/intellect/additional_modules/face_recognition/

9. http://www.secnews.ru/foreign/16309.htm.

10. http://itcrumbs.ru/google-ne-budet-raspoznavat-litsa_4444.

11. http://anasrat.ru/blog/50.html.
12. http://www.digimedia.ru/articles/digital- tales/bezopasnost/
13. http://www.gadgets.ru/2011/04/01/predator.
14. http://nnm.ru/blogs/Dus777/luxand_blink_1_0_rc.
15. Saidaminxo'dja Zoirxo'dja o'gli., Abdazimov ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari //Central Asian Research Journal for Interdisciplinary Studies (CARJIS). – 2022. – Т. 2. – №. 5. – С. 109-115.
16. Мирзаева М. Б., Абдазимов С. З. Использование технологий искусственного интеллекта в сфере высшего образования. – 2022.