COMPARATIVE ANALYSIS OF BIOMETRIC RECOGNITION TECHNIQUES

Javlonbek Bahodir ogli Uralov ,
Graduate student of the Urganch branch of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
E-Mail: javlonbekuralov0001@gmail.com
Nizomiddin Uktam ogli Zaripov ,
Graduate student of Tashkent University of Information Technologies named after Muhammad al-Khwarazmi
E-mail: nizomiddinzaripov@yandex.com

Abstract. The main task of this article is to provide a comparative analysis of currently widely used biometric authentication methods and to propose a high-performance method. That is, to determine the authentication method that is superior in all respects and can be used in various conditions and meets the requirements in terms of price and reliability.

Keywords: Biometric, face recognition, fingerprint, palm, print, voice, signature, authentication, identification, light, noise, time, price, reliability.

INTRODUCTION

The use of the Internet and high technologies has become one of the usual needs of people today. Currently, due to the increase in the amount of information circulating around the world, its beneficial and harmful aspects are also visible. it is necessary not to ignore the measures. At this point it should be said that today there is an opportunity to keep the confidentiality of information through various biometric authentication methods and technical means. Information is protected by methods of cryptographic protection of information known to us.

Security is an aspect that we face every day in our life. This must be a picture for the "Digital world", because every user's computer can be the object of a hacker attack. Recently, biometric authentication, which allows for reliable authentication of the user by measuring the physiological parameters and characteristics of a person, is becoming widespread.

Biometric authentication methods have the following advantages over traditional methods:

- Due to the uniqueness of biometric signs, the level of reliability of authentication is high;
-Difficulty of falsification of biometric symptoms;

During the implementation of biometric authentication methods, based on the signs that belong only to the person and are not found in other persons, who is the person and if he is registered, analyzing all the information about him, he really belongs to this enterprise or organization. is a system that identifies a person. For this reason, the use of biometric methods in the authentication of users in information systems and the selection of a suitable biometric method for a specific information system among them is one of the urgent tasks.

Types of commonly used biometric authentication methods

"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

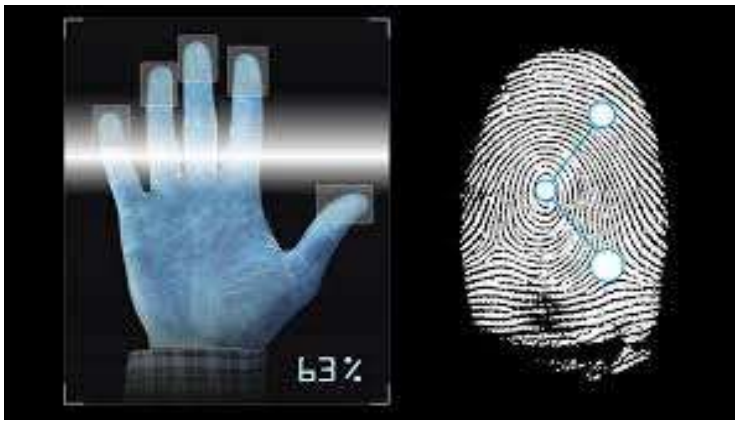
ISSN 2181-2632 www.involta.uz

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. This creates a unique capacitor.

Among the biometric authentication systems, the most common and popular
one is fingerprint identification and authentication. This system is said to be the "Dactyloscopic" method of biometric authentication.

Figure 1. Fingerprint scanning.



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

- Using ultrasounds;
-Using optical beams (FTIR);
- Using a semiconductor; [1]

Authentication by facial structure. Facial structure authentication differs in that it can be used everywhere because it is inexpensive and all computers have video capabilities. This system is mainly used for remote identification. The dimensions of the face are calculated based on the points in the figure below (Fig. 2). These points change due to fatness of the face. However, its structure, geometric dimensions and angles do not change when the face is fat or when it loses weight. Therefore, this system is considered one of the most reliable.

Here, the dimensions of its following points are obtained:

-The structure of the lip is its angle;
-Nose tip and dimensions;

ISSN 2181-2632 www.involta.uz

- 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 data warehouse, and it shows whether it is a person working in the institution or not. [2]

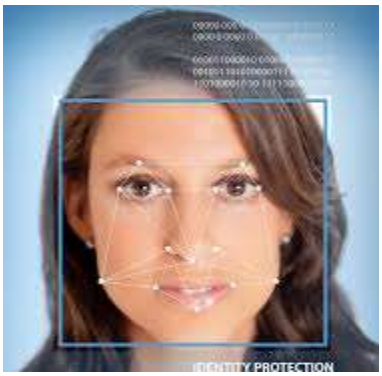


Figure 2. Authentication by facial structure.

In the case of the picture, mainly 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.

Retina authentication. The method of authentication using the retina is mainly carried out in two different ways.

1. Arc of the eye;
2. Location of blood vessels of the retina;

Authentication using the arc of the eye is mainly authenticated by the radius of the arc of the eye and its dimensions. The following picture shows the method of authentication by taking the radius of the arc of the eye and the dimensions of its location.

Authentication using the arc of the eye is more complicated and takes a significant amount of time. The cases of eye closure during work with blood vessels cause a number of problems in the authentication process.[3]

This biometric authentication method is considered to be at the highest level of security. From this bios, this biometric authentication method is placed in the offices of the states that need to ensure a high level of security.

Eye authentication hardware device developed by Biolink. It has been found that the location of the vessels in the retina is very different even in twins, but since the circle of the eye is similar to each other in some people, 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. [4]

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 various structures and statistical characteristics of the voice. From this bios, its problem can vary depending on the voice of a person: vocal health, age, mood, etc.

ISSN 2181-2632 www.involta.uz

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.

Palm authentication. Palm recognition confirms the geometry of a person's hand. This method is one of the fastest biometric authentication methods and is ideal for businesses that have tons of customers stopping by every day. Like fingerprints, the location of veins on the palms varies from person to person.[5]

Authentication using a signature. Signature recognition is an example of behavioral biometrics that identifies an individual based on their handwriting. It can be used in two ways:

• Static: In this mode, users write their signature on paper and after the writing is done, it is digitized by an optical scanner or camera to convert the signature image into bits.

	Fingerprint	**Face**	**Palm**	**Iris**	**Voice**	**Signature**
Light	3	1	3	2	3	3
catch a cold	3	2	3	2	2	3
Noise	3	3	3	3	2	3
Reliability	2	2	2	3	1	2
Cost	2	3	2	2	2	2
Time	3	2	2	2	2	2
Total:	**16**	**13**	**15**	**14**	**12**	**15**

• Dynamic: In this mode, users type their signature on a digital tablet, which captures the signature in real time. Users can sign using the appropriate pen. [6]

Comparative analysis of biometric authentication methods During the analysis of biometric authentication methods, we should pay special attention to its convenience in terms of time, health, and money. In the case of biometric authentication with the help of a fingerprint, it is mainly necessary that it is not injured and that it is placed correctly in the camera during scanning, in the case of biometric authentication with the help of the face, whether there are glasses on the face or not, the hairstyle does not fall on the face, in the case of biometric authentication with the help of voice, the sound of the voice ton, special attention should be paid to the state of the eye in biometric authentication using the eye.

In the table below, we consider the comparative analysis of biometric authentication methods.

This table is based on a numerical scoring system. Because these numbers are estimated based on general statistics.

In a 3-point system, i.e. (3 points - highly effective; 2 points - moderately effective; 1 point - low effective), we evaluate each biometric authentication method.

ISSN 2181-2632 www.involta.uz

The total result shows that the biometric authentication method with the help of a finger has the highest score. Its score is 16 points.

CONCLUSION

Nowadays, computer and communication technologies are developing rapidly day by day. For this reason, it would not be a mistake to say that there is no field left where computer technology has not penetrated. 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. When ensuring information security with the help of biometric methods, the first question that is put to us is which biometric method, at what price and for how many persons, and we should come to a clear conclusion about how we can install it in an enterprise, organization or institution. 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. It should be mentioned at the right time that every enterprise, organization or institution should thoroughly think about its security system and this security system should satisfy it in all aspects.

REFERENCES

1. R. Jantz (1987), ―Anthropological Dermatoglyphic Research, Annual Review of Anthropology, Vol. 16, Pp. 161–177.

2. Wing (1998), ―Overview of all INS Biometrics Projects, Proceedings of CTST’98, Pp. 543–552.

3. J. Markowitz (1999), ―Voice Biometrics: Speaker Recognition Applications and Markets‖, Voice Europe 1999: European Symposium on Voice Technologies, London.

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

5. Decision of the President of the Republic of Uzbekistan " O‘zbekiston Respublikasining Milliy axborot-kommunikatsiya tizimini yanada rivojlantirish chora-tadbirlari to‘g‘risida ". June 27. 2013.

6. Ganiev S. K., Karimov M. M. " Hisoblash sistemalari va tarmoqlarida informat-siya himoyasi ": a study guide for students of higher educational institutions. - Tashkent

ISSN 2181-2632 www.involta.uz