ISSN: 2707-8965 (Online) & 2708-3772 (Print)

Volume: 3, Issue: 6
Page: 103 - 118
2021

Euro Afro Studies International Journal®
(EASIJ.COM)

Security levels of current biometric identification

Author(s), O'RINOV NODIRBEK TOXIRJONOVICH,
ABDURXMANOV JAMOLIDIN KOMOLDINOVICH,
AND
OLIMOV MUSLIMBEK ULUG'BEK O'G'LI

EASIJ
Accepted 15 June 2021
Published 30 June 2021
DOI: 10.5281/zenodo.5048324

Abstract:

The problem of minimizing the possibility of obtaining unauthorized access to information is investigated. The concept of the authentication process and its types are considered. Described are static and dynamic biometric authentication methods based on the use of biometric characteristics such as fingerprint, iris, retina, hand geometry, face geometry, face thermogram, voice and handwriting. The advantages of dynamic methods of biometric authentication are revealed. Based on the results of the analysis of these methods, it was proposed to use facial expressions as a biometric characteristic. It is concluded that the most modern and promising method of biometric authentication is the assessment of the emotional state and facial expressions through constant covert monitoring using a web camera. The prospect of research in the development of this method of bio-metric authentication is the development of a mathematical apparatus, methods and technologies of algorithmic, information and software in this subject area. The development of the mathematical apparatus should be based on the use of methods of local binary templates and nearest neighbors. The method based on the assessment of the emotional state and facial expressions is the most promising, however, research in this area is currently at the stage of development, which does not give a complete picture of all the possibilities of applying the method.

Keywords: identification, authentication, biometric authentication, biometric characteristics, static methods, dynamic methods,

About Author

Author(s): O'RINOV NODIRBEK TOXIRJONOVICH,

Teacher, Department of Information Technology, Andijan State University, Uzbekistan.
E-mail: nodirbekurinov1@gmail.com

ABDURXMANOV JAMOLIDIN KOMOLDINOVICH

Candidate of physical and mathematical sciences, Department of Information Technology, Andijan State University, Uzbekistan.
E-mail: jamolidinkamol@gmail.com

OLIMOV MUSLIMBEK ULUG'BEK O'G'LI

Teacher, Department of Information Technology, Andijan State University, Uzbekistan.
E-mail: ochilov92@list.ru

1. Introduction

Modern authentication methods include biometric-based authentication. With biometric authentication, the user's secret data can be both the retina and the fingerprint. These biometric images are unique for each user, which provides a high level of protection for access to information. According to pre-established protocols, the user's biometric samples are registered in the database.

Modern biometric authentication is based on two methods:

- static authentication method - recognizes the physical parameters of a person that he possesses throughout his life: from his birth to death (fingerprints, distinctive characteristics of the iris, drawing of the retina, thermogram, face geometry, geometry of the hand and even a fragment of the genetic code);
- dynamic method - analyzes the characteristic features, features of user behavior, which are demonstrated at the moment of performing any ordinary daily action (signature, keyboard handwriting, voice, etc.).

The main biometric security market in the world has always been the static method. Dynamic authentication and combined information security systems occupied only 20% of the market. However, in recent years, there has been an active development of dynamic protection methods. Of particular interest in network technologies are keyboard handwriting and signature authentication methods.

In connection with the rather rapid development of modern biometric technologies, a critical problem appears - the definition of general standards for the reliability of biometric security systems. Means with quality certificates issued by the International Computer Security Association ICSA (International Computer Security Association) enjoy great authority among specialists.

2. Related work

2.1 Static biometric authentication method and its variants

Fingerprinting is the most popular biometric authentication technology based on scanning and recognizing fingerprints.

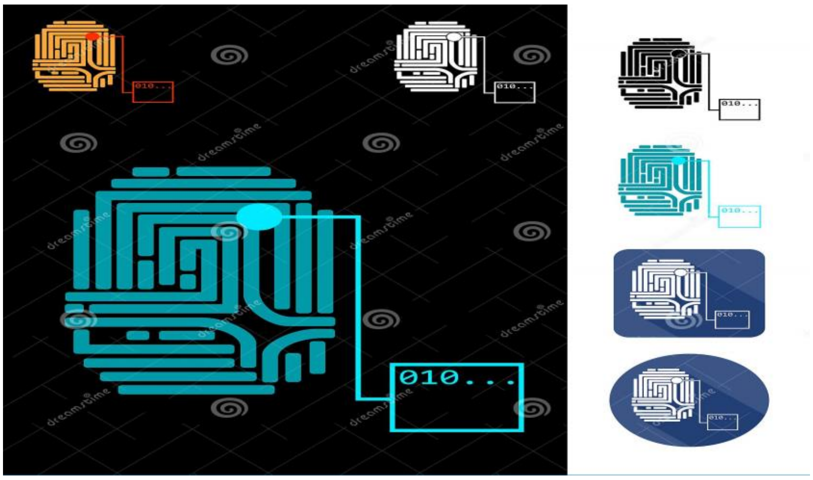

Figure 1. Fingerprinting

This method is actively supported by law enforcement agencies in order to attract electronic samples to their archives. Also, the fingerprint scanning method is easy to use and reliable due to the versatility of the data. The main device of this biometric authentication method is a scanner, which itself is small in size and relatively inexpensive in price. Such authentication is carried out rather quickly due to the fact that the system does not require recognition of each line of the pattern and its comparison with the original samples in the database. It is enough for the system to detect coincidences in scale blocks and analyze bifurcations, breaks and other distortions of lines (minutiae).

The uniqueness of each fingerprint allows this method of biometric authentication to be used both in forensics, in the processes of serious business operations, and in everyday life. Recently, there have been many laptops with built-in fingerprint readers, keyboards, computer mice, and smartphones for user authentication.

There are also downsides to this seemingly undeniable and not fake authentication. Due to the use of sophisticated algorithms for recognizing the smallest papillary lines, the authentication system can show failures if there is insufficient contact between the finger and the scanner. It is also possible to deceive the means of authentication and the protection system itself with the help of a dummy (very well made) or a dead finger.

According to the principle of operation, the scanners used for authentication are divided into three types:

- optical scanners operating on reflection technology, or on the principle of lumen. Of all types, optical scanning is not capable of recognizing a dummy, however, due to its cost and simplicity, it is optical scanners that are most popular;
- semiconductor scanners - categorized into RF, capacitive, temperature-sensitive, and pressure-sensitive scanners. Thermal (thermal) and RF scanners are the best at recognizing a real fingerprint and preventing fingerprint authentication. Semiconductor scanners are considered more reliable than optical scanners;
- ultrasound scanners. This type of device is the most complex and expensive. With the help of ultrasound scanners, you can authenticate not only by fingerprints, but also by some other biometric parameters, such as heart rate, etc.

2.2 Retinal authentication. This method began to be used back in the 50s of the last century. At that time, just the uniqueness of the pattern of the blood vessels of the fundus was studied and determined.

Retinal scanners are rather large and more expensive than fingerprint scanners. However, the reliability of this type of authentication is much higher than fingerprinting, which justifies the investment. Features of the pattern of the blood vessels of the fundus are such that it does not repeat even in twins. Therefore, such authentication has maximum security. It is almost impossible to deceive the retinal scanner. Failures in eye pattern recognition are negligible - about one in a million cases. If the user does not have serious eye diseases (for example, cataracts), he can confidently use the retinal authentication system to protect access to all kinds of storages, private offices and top-secret objects.

Retinal scans use low-intensity infrared radiation that is directed to the blood vessels of the fundus through the pupil. The signal displays several hundred characteristic points, which are written into the template. The most modern scanners aim a soft laser instead of infrared light.

To pass this authentication, a person must bring his face as close as possible to the scanner (the eye must be no more than 1.5 cm from the device), fix it in one position and direct his gaze to the scanner display, to a special mark. Near the scanner, in this position, you have to be for about a minute. This is how much time it takes for the scanner to carry out the scanning operation, after which the system will need a few more seconds to compare the received sample with the established template. Long stay in one position and fixation of a glance at a flash of light are the biggest disadvantages of using this type of authentication. Plus, due to the relatively long retinal scanning and processing of the results, this device cannot be installed to authenticate a large number of people (for example, a checkpoint).

2.3 Iris authentication. This authentication method is based on recognizing the unique features of the iris.

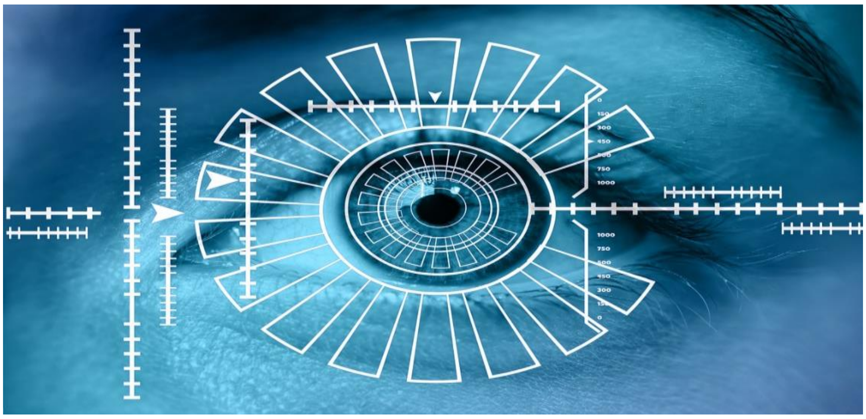

Figure 2. Iris authentication.

A network-like, complex pattern of a movable diaphragm between the posterior and anterior chambers of the eye is the unique iris. This drawing is given to a person even before his birth and does not change much throughout his life. The reliability of authentication by scanning the iris of the eye is facilitated by the distinction between the left and right eyes of a person. This technology practically eliminates errors and failures during authentication.

However, it is difficult to call devices that read iris patterns - scanners. This is most likely a specialized camera that takes 30 pictures per second. Then one of the records is digitized and converted into a simplified form, from which about 200 characteristic points are selected, and information on them is written into a template. This is much more reliable than scanning fingerprints - only 60-70 characteristic points are used to form such patterns.

This type of authentication implies additional protection against fake eyes - in some device models, to determine the "life" of the eye, the flow of light directed into it changes and the system monitors the reaction and determines whether the pupil size changes.

These scanners are already widely used, for example, in the airports of many countries to authenticate employees when crossing restricted areas, and have also proven themselves well in England, Germany, the USA and Japan during experimental use with ATMs. It should be noted that in iris authentication, in contrast to retinal scanning, the reading camera can be located from 10 cm to 1 meter from the eye and the scanning and recognition process is much faster. These scanners are more expensive than the aforementioned biometric authentication tools, but recently they are becoming more available.

2.4 Authentication by hand geometry - this method of biometric authentication involves measuring certain parameters of the human hand, for example: length, thickness and curvature of fingers, general structure of the hand, distance between joints, width and thickness of the palm.

Figure 3. Authentication by hand geometry.

Human hands are not unique, therefore, for the reliability of this type of authentication, it is necessary to combine recognition by several parameters at once.

The probability of errors in recognizing the geometry of the hand is about 0.1%, which means that in case of bruises, arthritis and other diseases and injuries of the hand, it is most likely that authentication will fail. So, this method of biometric authentication is not suitable for ensuring the security of objects with a high degree of secrecy.

However, this method has become widespread due to the fact that it is user-friendly for a variety of reasons. One of such important reasons is that the device for recognizing the parameters of the hand does not force the user to discomfort and does not take much time (the entire authentication process is carried out in a few seconds). Another reason for the popularity of authentication based on hand geometry is the fact that neither temperature, nor dirtiness, nor humidity of the hand affects the authentication procedure. Also, this method is convenient because for brush recognition you can use a low quality image - the size of the template stored in the database is only 9 bytes. The procedure for comparing a user's brush with an established template is very simple and can be easily automated.

Devices of this type of biometric authentication can have different appearance and functionality - some scan only two fingers, others take a picture of the whole hand, and some modern devices use an infrared camera to scan veins and perform authentication based on their image.

This method was first used in the early 70s of the last century. Today, such devices can be found at airports and various enterprises, where it is necessary to generate reliable information about the presence of a particular person, time attendance and other control procedures.

2.5 Face geometry authentication. This biometric authentication method is one of the "three big biometrics" along with iris recognition and fingerprint scanning.

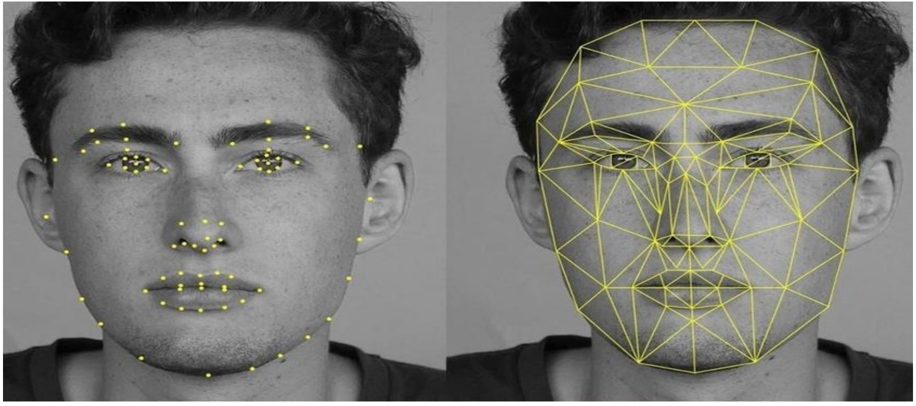

Figure 4. Face geometry authentication.

This authentication method is divided into 2D and 3D recognition. Two-dimensional (2D) face recognition has been used for a very long time, mainly in forensic science. But, every year this method is being improved, thereby increasing the level of its reliability. However, the two-dimensional method of face recognition is still far from perfect - the probability of false positives with this authentication varies from 0.1 to 1%. The frequency of non-recognition errors is even higher.

Much more hopes are pinned on the newest method - three-dimensional (3D) face recognition. The reliability estimates of this method have not yet been derived, since it is relatively young. About ten leading global IT companies, including those from Russia, are developing 3D face recognition systems. Most of these developers provide scanners with their software to the market. And only a few are working on the creation and release of scanners.

In three-dimensional face recognition, many complex algorithms are used, the effectiveness of which depends on the conditions of their application. The scanning procedure takes about 20-30 seconds. At this moment, the face can be rotated relative to the camera, which forces the system to compensate for movements and form a projection of the face with a clear selection of facial features, such as the contours of the eyebrows, eyes, nose, lips, etc. Then the system determines the distance between them. Basically, the template is composed of such unchanged characteristics as the depth of the eye sockets, the shape of the skull, eyebrows, the height and width of the cheekbones and other pronounced features, thanks to which the system will subsequently be able to recognize the face even with a beard, glasses, scars, headgear, etc. other things. In total, from 12 to 40 features of the user's face and head are used to build a template.

The International Subcommittee on Biometrics Standardization (IS0 / IEC JTC1 / SC37 Biometrics) has recently been developing a unified data format for human face recognition based on 2D and 3D images. Most likely, these two methods will combine you into one biometric authentication method.

2.6 Facial thermography. This biometric authentication method is expressed in the identification of a person by his blood vessels.

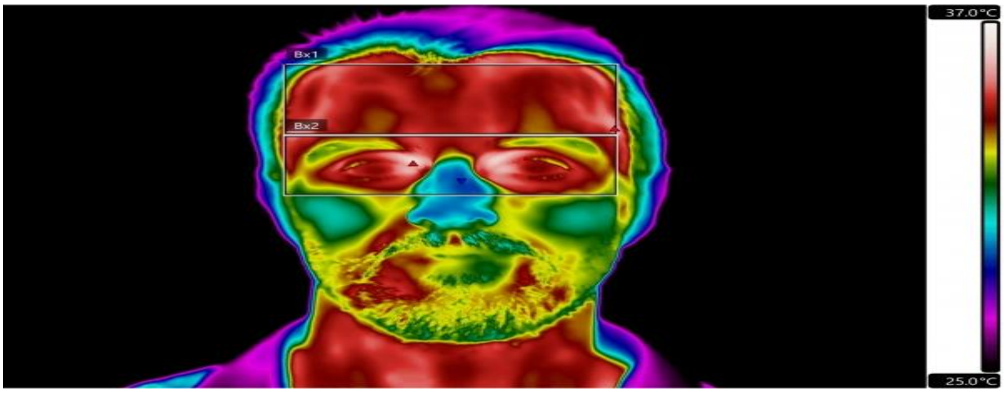

Figure 5. Facial thermography

The user's face is scanned using infrared light and a thermogram is formed - a temperature map of the face, which is quite unique. This method is comparable in reliability to the fingerprint authentication method. Face scanning with this authentication can be performed from a ten-meter distance. This method is able to recognize twins (as opposed to recognition by the geometry of the face), people who have undergone plastic surgery, using masks, and it is also effective, despite the body temperature and aging of the body.

However, this method is not widespread, possibly due to the low quality of the received thermograms of faces.

3. Dynamic biometric authentication methods

3.1. Voice recognition method. Biometric method of user authentication by voice is the most accessible for implementation.

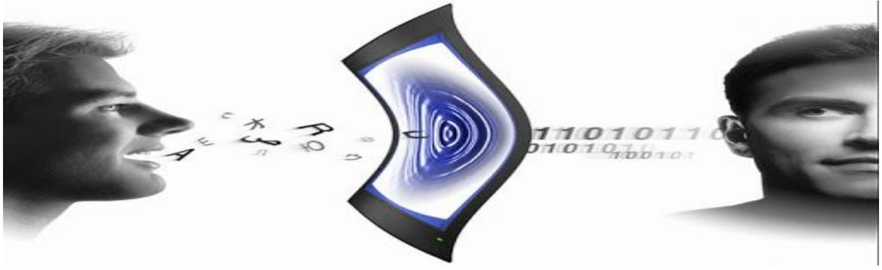

Figure 6. Voice recognition method

This method allows identification and authentication of a person using only one microphone, which is connected to the recording device. The use of this method is useful in court cases, when the only evidence against a suspect is a recording of a telephone conversation. The voice recognition method is very convenient - the user just needs to say a word, without performing any additional actions. And finally, the huge advantage of this method is the right to perform hidden authentication. The user may not always be aware of the inclusion of additional verification, which means that it will be even more difficult for attackers to gain access.

The formation of a personal template is carried out according to many characteristics of the voice. This can be the tonality of the voice, intonation, modulation, distinctive features of the pronunciation of some speech sounds, and more. If the authentication system has properly analyzed all of the voice characteristics, then the likelihood of a stranger being authenticated is negligible. However, in 1-3% of cases, the system can give a refusal to the present owner of a previously defined vote. The fact is that a person's voice can change during an illness (for example, a cold), depending on the mental state, age, etc. Therefore, it is undesirable to use the biometric voice authentication method in high-security facilities. It can be used to access computer labs, business centers, laboratories and similar security facilities. Also, voice recognition technology can be used not only as authentication and identification, but also as an irreplaceable assistant in voice data input.

3.2. The keyboard handwriting recognition method is one of the most promising biometric authentication methods today. Keyboard handwriting is a biometric characteristic of the behavior of each user, namely, the input speed, the time the keys are held, the intervals between keystrokes, the frequency of typing errors, the number of overlaps between the keys, the use of function keys and combinations, the level of arrhythmia when typing, etc.

Figure 7. The keyboard handwriting recognition method.

This technology is universal; however, it is best suited for authenticating remote users. Both foreign and Russian IT companies are actively involved in the development of keyboard handwriting recognition algorithms.

Authentication by user's keyboard handwriting has two ways:

- entering a known phrase (password);
- input of an unknown phrase (randomly generated).

Both authentication methods involve two modes: learning mode and authentication mode itself. The training mode consists in the user entering a code word (phrase, password) multiple times. In the process of redialing, the system identifies the characteristics of text input and generates a template for user metrics. The reliability of this type of authentication depends on the length of the phrase entered by the user.

Among the advantages of this authentication method should be noted the ease of use, the ability to carry out the authentication procedure without special equipment, as well as the possibility of hidden authentication. The disadvantage of this method, as in the case of voice recognition, is the dependence of the system failure on age factors and the user's health. After all, motor skills, much stronger than the voice, depend on the state of the person. Even simple human fatigue can affect authentication. Changing the keyboard can also be the reason for the system failure - the user is not able to immediately adapt to the new input device and therefore, when entering a test phrase, the keyboard handwriting may not match the template. In particular, it affects the rate of entry. Although, researchers suggest increasing the effectiveness of this method through the use of rhythm. Artificially adding a rhythm (for example, a user typing a word to some familiar melody) ensures the stability of the keyboard handwriting and more reliable protection from intruders.

3.3. Verification of a signature. Due to the popularity and widespread use of various touch screen devices, the biometric signature authentication method is becoming very popular.

Figure 8. Verification of a signature.

The most accurate verification of the signature is ensured by the use of special light pens. In many countries, electronic documents signed with a biometric signature have the same legal force as paper media. This allows you to carry out document flow much faster and more smoothly. In Russia, unfortunately, only a paper signed document, or an electronic document with an officially registered electronic digital signature (EDS), is trusted. But, EDS is easy to transfer to another person, which cannot be done with a biometric signature. Therefore, verification by biometric signature is more reliable.

Biometric signature authentication has two methods:

- based on the analysis of the visual characteristics of the signature. This method assumes a comparison of two signature images for identity matching - this can be done both by the system and by a person;
- a method of computer analysis of the dynamic characteristics of writing a signature. Authentication in this way occurs after a thorough examination of the information about the signature itself, as well as about the statistical and periodic characteristics of its writing.

Formation of the signature template is carried out depending on the required level of protection. In total, one signature is analyzed for 100-200 characteristic points. If, however, the signature is made using a light pen, then in addition to the coordinates of the pen, the angle of its inclination and the pressure of the pen are also taken into account. The angle of the pen is calculated relative to the tablet and clockwise.

This method of biometric authentication, as well as recognition of keyboard handwriting, have a common problem - dependence on the psychophysical state of a person.

4. Combined Biometric Authentication Solutions

A multi-modal or combined biometric authentication system is a device that combines several biometric technologies at once.

Combined solutions are rightfully considered the most reliable in terms of protecting information using the user's biometric indicators, because it is much more difficult to fake several indicators at once than one sign, which is practically beyond the power of attackers. The combinations "iris + finger" or "finger + hand" are considered to be the most reliable.

Figure 9. Combined Biometric Authentication Solutions.

Although, recently, systems like "face + voice" are gaining popularity. This is due to the widespread use of communication tools that combine the modalities of audio and video, for example, mobile phones with built-in cameras, laptops, video intercoms, and so on.

Combined biometric authentication systems are much more efficient than monomodal solutions. This is confirmed by many studies, including the experience of one bank, which first installed a user authentication system by face (error rate due to low quality cameras 7%), then by voice (error rate 5% due to background noise), and then, by combining these two methods, they have achieved almost 100% efficiency.

Biometric systems can be combined in various ways: in parallel, sequentially, or according to a hierarchy. The main criterion when choosing a method for integrating systems should be minimizing the ratio of the number of possible errors to the time of one authentication.

In addition to combined authentication systems, multifactor systems can also be used. In systems with multi-factor authentication, the user's biometric data is used together with a password or electronic key.

5. Biometric data protection

The biometric authentication system, like many other security systems, can be attacked by intruders at any time. Accordingly, since 2011, international standardization in the field of information technology provides for measures to protect biometric data - standard IS0 / IEC 24745: 2011. In uzbeks whom the legislation protecting biometric data regulates the national legislation database "On personal data".

The most common direction in the field of modern biometric authentication methods is the development of strategies for protecting stored biometric templates in databases. Identity theft is considered to be one of the most popular cybercrimes of today all over the world. Leaking templates from the database makes crimes more dangerous, since it is easier for an attacker to recover biometric data by reverse engineering the template. Since biometric characteristics are integral to its carrier, a stolen template cannot be replaced with an uncompromised new one, unlike a password. The danger of stealing a template also lies in the fact that in addition to accessing protected data, an attacker can obtain secret information about a person, or organize secret surveillance.

The protection of biometric templates is based on three main requirements:

- irreversibility - this requirement is focused on saving the template in such a way that it would be impossible for an attacker to computationally recover the biometric characteristics from the sample, or create physical forgeries of biometric features;
- discernibility - the accuracy of the biometric authentication system must not be compromised by the template protection scheme;
- cancellation - the ability to generate several protected templates from one biometric data. This property provides the biometric system with the ability to revoke biometric templates and issue new ones when data is compromised, and also prevents the comparison of information between databases, thereby preserving the privacy of user data.

When optimizing strong template protection, the main challenge is to find an acceptable understanding between these requirements. The protection of biometric templates is based on two principles: biometric cryptosystems and the transformation of biometric traits. Recent changes in the legislation prohibit the operator of the biometric system independently, without the presence of a person, to change his personal data. Accordingly, systems storing biometric data in encrypted form become acceptable. This information can be encrypted in two ways: using a regular key and encryption using a biometric key - access to data is provided exclusively in the presence of the owner of the biometric indicators. In conventional cryptography, the decryption key and the encrypted template are two completely different units. A template can be considered secure if the key is protected. The biometric key simultaneously encapsulates the cryptographic key template. In the process of encryption in this way, only partial information from the template is stored in the biometric system. It is called a secure sketch. The original template is restored based on the protected sketch and another biometric sample similar to the one presented during registration.

IT professionals researching biometric template protection schemes have identified two main methods for creating a secure thumbnail:

- fuzzy commitment;
- fuzzy vault.

The first method is suitable for protecting biometric templates in the form of binary strings of a certain length. And the second can be useful for protecting patterns, which are collections of points.

The introduction of cryptographic and biometric technologies has a positive effect on the development of innovative solutions to ensure information security. Especially promising is multifactor biometric cryptography, which combines the technologies of threshold cryptography with secret sharing, multifactor biometrics and methods for converting fuzzy biometric features into basic sequences.

It is impossible to form an unambiguous conclusion which of the modern biometric authentication methods, or combined methods is the most effective for those or other commercial ones, based on the ratio of price and reliability. It is clearly seen that for many commercial tasks, it does not seem logical to use complex combined systems. But, not at all to consider such systems is also not true. The combined authentication system can be used taking into account the currently required security level with the possibility of activating additional methods in the future.

Conclusion

Based on the results of the review and analysis of modern methods of biometric authentication, it can be concluded that the method based on the assessment of the emotional state and facial expressions is the most promising, since its use reduces the likelihood of errors of the first and second kind, thereby increasing the security of information systems. It is still difficult to get a complete idea of all the possibilities of using this method, due to the fact that research in this area is currently at the stage of development.

LIST OF REFERENCES

Nyrkov A. P. Multiservice network of the transport industry / A. P. Nyrkov, S. S. Sokolov, S. Belousov // Vestn. computer and information technology. 2014. No. 4 (118). S. 33-38.

Nyrkov A. P. Ensuring the safe functioning of a multiservice network of the transport industry / A. P. Nyrkov, S. S. Sokolov, A. S. Belousov // Dokl. Tomsk. state Univ management and pa - dioelektroniki. 20 l 4.No. 2 (32). S. 143-149.

Global research on information security. Prospects for 2015 // URL: http: //www. pwc.ru /ru/riskassurance/publications/managing - cyberrisks. html (drawn date - Nia: 28/03/2016).

Methods and means of protection against unauthorized access // URL: http: // www. panasenko.ru / Articles / 77/77. html (date accessed: 03/31/2016).

Identification and authentication, access control//URL: http://citforum. ru/security/articles/galatenko (date accessed: 03/27/2016).

The biometric authentication system//theURL: https://ru.wikipedia.org/wiki/Biometricheskie_ sistemy_autentifikatsii #

Gureeva O. Biometricfingerprint identification. Technology FingerChip // Compo - nents and technology. 2007. No. 4 p. 176-180 // URL: http://www.kit-e.ru/assets/files/pdf/2007_04_176.pdf.

Retinal authentication methods // URL: https: // habrahabr. ru / the post / 261309 / (drawn date - Nia: 01/04/2016).

Dynamic methods of biometric identity authentication // URL : http : // re . mipt . ru / infsec / 2006 / essay / 2006_ Dynamic _ biometric _ authentification Cherkezov . pdf (date of access: 28.03.2016).

Schemelinin VL Investigation of the stability of voice verification to attacks using the synthesis system / VL Schemelinin , KK Simonchik // Izv . higher . study. Head . Instrumentation. 2014. T. 57, No. 2. S. 84-88.

Tass KL method of human identification by voice / KL Tasso, R. A. Woodpeckers // Engineer - ny magazine: Science and Innovation. 2013. Issue . 6 // URL: http://engjournal.ru/catalog/it/biometric/1103.html.

Vyskub V. G. Possibilities of increasing the accuracy of biometric recognition systems / G. Vyskub , I. V. Prudnikov // Engineering Physics. 2009. Issue . 5.S. 41-43.

Markelov KS Biometric information technology: current and future IU - Toda / KS Markelov, Vladimir Nechayev // Information and telecommunication technologies. 2013. No. 18. S. 24-42.

Shibanov S. V. Comparative analysis of modern methods of user authentication / V. Shibanov, D. A. Karpushin // Mathematical and software systems in industrial and social spheres. 2015. No. 1. S. 33-37.

Mayorov AV Features of technology of biometric protection of software / AV Mayorov // Scientific and technical. conf . young specialists of FSUE "PNIEI". Penza, 2009.7 p.

Ekman P. Psychology of emotions. I know how you feel / P. Ekman . SPb .: Peter, 2010.180 p.

GOST R ISO / IEC 197194-5-2006. Automatic identification. Identification biometriche – Skye. Biometric data exchange formats. Part 5. Face image data // URL: http : // snipov . net / database / c _3944567195_ doc _4293849863. html.

Hamsters M. Yu Principles of the software package for modeling systems by recognizing – Niya face images / M. Yu Khomyakov, GA Kuharev // Math . St. Petersburg. state electrotechnical. university "LETI". 2010. No. 7.S.41-46.

Nodirbek O'rinov, Faxriddin Madolimov, Aliyeva Gulzira, and Umarova Ra'no. "Biometrics authentication: A study." ACADEMICIA: An International Multidisciplinary Research Journal 10.5 (2020): 210-214.

Cite this article:

Author(s), O'RINOV NODIRBEK TOXIRJONOVICH, ABDURXMANOV JAMOLIDIN KOMOLDINOVICH, AND OLIMOV MUSLIMBEK ULUG'BEK O'G'LI, (2021). "Security levels of current biometric identification", **Name of the Journal:** Euro Afro Studies International Journal, (EASIJ.COM), P, 103 –118. DOI: www.doi.org/10.5281/zenodo.5048324 , Issue: 6, Vol.: 3, Article: 10, Month: June, Year: 2021. Retrieved from https://www.easij.com/all-issues/

Published By

AND

ThoughtWares Consulting & Multi Services International (TWCMSI)