

The Role of Biometric Technology in Information Security

Tofiq Kazimov¹, Shafagat Mahmudova²

^{1,2}*Institute of Information Technology of ANAS, Baku, Azerbaijan*

Abstract - *The article is about the role of biometric technology in information security. The increased terrorist threat in the world has urged the biometric identification systems to be established in order to improve the safety systems. The advantages of biometric technology are shown to address the issues facing the authorities of law enforcement system, the state security system and the defense guarantee of the country on a national basis. The recommendations are given in this area.*

Key words: *information security, biometric technology, biometric signs, terrorism*

1. INTRODUCTION

The dynamic scientific and technical progress, which causes everyone's surprise, opens a wide range of opportunities for the development of biometric technologies. The technology has a very important role in preventing dangerous incidents. Biometric identification technology is one of the effective tools to detect and overcome the criminals.

The use of biometric technologies provides reliable verification of the passengers crossing state borders, and strengthens the control of passport and visa regulations, and other identification documents. The recognition systems are of particular importance here. In addition to the criminal law system, it is widely used in other areas. Leading research institutions around the world conduct researches in this regard. Azerbaijan takes measures against dangerous phenomena, and develops state programs, as well. The relevant agencies of Azerbaijan National Academy of Sciences (ANAS), which are integrating into the world science, provide permanent scientific support to the state programs adopted by the state president. And the new tasks arisen from the **adoption of the "State Program on the development of biometric identification system in the Republic of Azerbaijan" are implemented by the scientists consistently.** Biometric technologies are widely used in security systems. The examples of biometric technologies are shown in Fig -1.

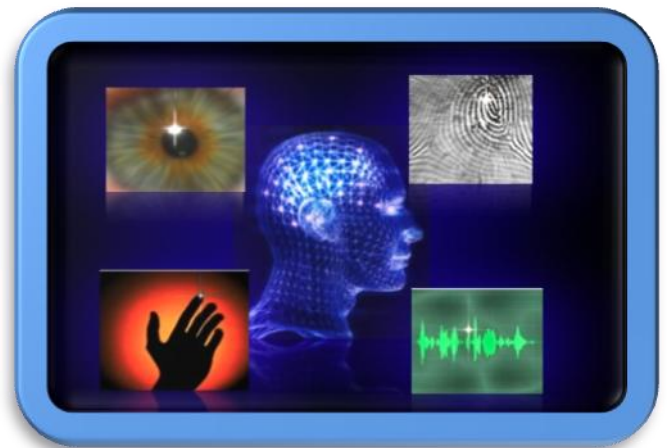


Fig -1: Examples of biometric technology

The main advantages of biometric technologies include high reliability, maximum protection from unauthorized access, and simplicity of use.

Various biometric technologies exist:

- eye iris identification technology;
- voice identification technology;
- fingerprint identification technology;
- hand patterns identification technology;
- image-based human face identification technology;
- deoxyribonucleic acid (DNA) identification technology, and so on.

Nowadays, biometric technologies are applied in different areas, from work entrance organization to the person identification during payment transactions. The use of new defense tools is of particular significance during e-business and banking transactions. Multimodal biometric technologies are used to improve identification in long-term studies; therefore, the control is carried out according to several biometric features, which enables to prevent an unauthorized access [1].

The use of biometric technology is indispensable for improving the security of various systems that require the user verification and the development of information technologies. Its use will prevent an unauthorized access to material objects and data reliably, as well as ensure efficient identification of a person.

Biometric technologies are applied in diverse areas: access to work places and network resources, information protection, providing access to certain resources, airport security and so on. Note that, implementation of e-business and e-government is possible with only identification of a person, i.e., without any other procedures.

The US Federal Bureau of Investigation (FBI) has announced the completion of the recognition of a new

biometric system. The data on tens of millions of US residents will be included in the system's database. Over time, such systems are expected to be developed in Russia. FBI Next Generation Identification (NGI) system collects and processes the data, and identifies the eyes, fingerprints and iris (Fig -1). The system responds to high level requests in real-time mode as soon as possible [2].

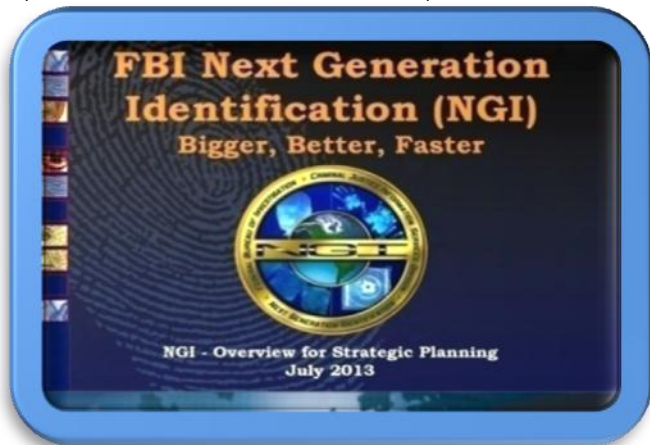


Fig -2. Next Generation Identification System

2. FIGHT AGAINST TERRORISM AND CRIMINALS

Traditionally, compared to various methods the biometric identification methods have a number of advantages:

- **biometric signs are very difficult to forge;**
- **reliability of biometric identification features is very high** for its uniqueness;
- **biometric identifiers can not be forgotten or lost** as passwords or credit cards.

Each biometric method has its advantages and disadvantages. Therefore, the recognition may not be achieved primarily through the use of any method every time.

Quantitative measurement of safety is very difficult. The increased terrorist threats and the need for improved security systems have led to the rapid increase in the volume of biometric equipment market in recent years. Not only commercial enterprises, as well as government departments are the largest customers of biometric systems. Special attention is paid to the airports, stadiums and other facilities, where the mass control is needed.

Since 2006, the citizens of European Union countries have had e-passports. And the biometric signs (finger prints, iris etc.), as well as other data of the citizens (insurance card numbers, driver license, bank accounts, etc.) are stored in the special microchips of those documents. The application areas of such documents are unlimited: international passports, credit cards, medical cards, insurance certificates, permission cards and so on.

In modern times, the fight against terrorism and crime has increased sharply.

The global wave of terrorist attacks has urged improvement of detection and preventive security systems. One of the major issues facing many countries is enabling new approaches and new principles for the development of various systems preventing smuggling and terrorist

attacks, and the organization of the centers for national security, and international integration.

The application of innovative technologies plays an important role in the present circumstances.

Perfection of the systems of search, detection, and the identification of crime initiators against the persons, society and state, in general, is of particular importance. The resolution of such issues requires new approaches and the use of modern technology globally. Any evidence obtained as the result of investigation or operative-search should be used within a real period of time efficiently [3]. National law enforcement system allows the state security system and defense agencies to solve a wide range of issues:

- Searching for the potential criminals or the persons suspected in the dangerous and illegal activities (citizens' lives, government agencies, etc.);
- Detection of the incident participants is one of the main tasks of law enforcement, public safety and defense system of the country;
- Successful resolution of these issues at the state level is possible through the use of biometric information technologies;
- Developing distributed system for the collection and storage of multimedia data (pictures, video records, etc.);
- Interactive search of suspects from the databases, which include the data collected as the result of investigations and operational-searches, and so on.

The data, criminal banks, and databases existing in the internal affairs agencies are quite messy and mostly of local effect. It causes certain difficulties in the fights against inter-regional criminals, which restricts the search opportunities to detect the suspects, that is, the identification process is not carried out.

The biometric features as voice and facial image of a person may be used for the solution of the problems (Fig -3).

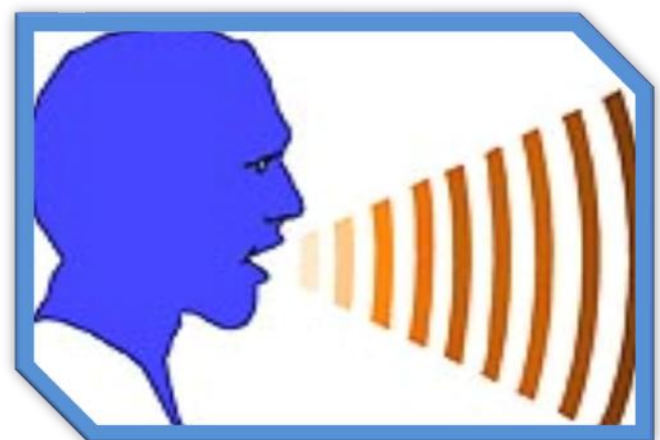




Fig -3: Voice and facial image of a person

Facial elements of each person are his individual biometric characteristics. The photos in the documents are widely used for the identification, and all the countries have adopted standards in this regard.

The advantages of biometric identification basin on photos are as follows:

- photo or video images of the face do not require a direct relation with the subject during the identification, and can be confidential;
- compared to other biometric databases the photos databases are complete and widespread;
- application of this changes technology is not related to the amendments of the laws;
- unique and relatively stable biological parameters of a person.

The integrated information system shall insure the national criminalistics to search and identification from data banks and databases:

- integrated biometric information system should be available for the search and detection of suspects;
- photo storage and processing ways, as well as the identification of these signs should be carried out within a short time;
- scenarios of the work of the law enforcement officials, which support the system, should be apparent;
- the identification process should be carried out close to real-time mode, and processing time of data entries should be minimal;
- biometric identification system should be available for the identification of a person basing on his image;
- The algorithms of the identification of a person basing on his image should be based on the assessment and the inspection results of the image quality;
- If the image processing problems are detected, it is transferred to the expert automatically. The expert can process it, or specify image control points, which increases the accuracy of the system [4].

3. AUTOMATIC IDENTIFICATION OF BIOMETRIC FEATURES OF FACIAL IMAGE

The algorithms of the identification of a person basing on the image select and generate the face models automatically. In this case, the distance between the pupils and the other features are listed. Selected features should be resistant to hairstyle changes, as well as wearing the glasses, and other transformations.

The advantage of realizing various biometric identification algorithms on a single platform includes that the results of all identification are given to the operator in a single form. Subsequently, the results transmission, their measurement and approaches to decision-making are designed for the organization of biometric identification algorithms.

Unified system of biometric search and national criminalities is formed in a functional level as follows:

1. Realizing the identification according to the data collection, registration cards and descriptions of wanted persons;
2. The data processing and storage, computing operations;
3. Organization of biometric data bank and registration cards database;
4. Definition of the search parameters, delivering the data obtained as the result of face detection, search results analysis expertise, and so on.

4. ENSURING SECURITY

A number of dangerous phenomena can be avoided through the use of biometric networks. Biometric networks can be used anywhere. In regard to the increase of terrorism in the world recently, people's attention is drawn to the security issues at the airports more and more. Governments, airlines, and airport administrations are concerned about the vulnerable problems and protection of public passenger and cargo transportation.

Focusing (the clear point of the object in taken photo) in security issues has led to a radical change in airport operations and their growth. Airlines and airport administrations, as well as federal government allow solving the problems and prefer high-level technology. Modern technologies are used not only for new operations, as well as for the work, which is not possible to perform manually.

Nowadays, scientific articles include lots of information about ensuring networks safety. The study of new devices and technologies is in the process, so that they are applied and developed at the airports. The articles in this field provide information about the face recognition systems, iris scanners, finger print identifiers, smart-cards, explosives detection systems, radio devices, and other new technologies [5].

One of the key issues of security systems is the air passenger safety, however, the airports, as a rule, are working independently of each other. The work of numerous suppliers is provided by the individual networks of new technologies, which requires installation of new equipments and expensive cable system for each of them.

In most airports the number of independent networks is so great that (sometimes more than 50), it prevents effective management. Most of these networks facilitate the functioning of numerous inspection cameras, X-ray systems, cargo scanning devices and access control systems properly. The number of networks is growing in the process of additional security systems extending. The lack of a single biometric network makes it difficult for local and federal law enforcement agencies to transfer the information inside and outside the airport.

Combination of new devices related to security shall be applied in order to gain the confidence of the air passengers, and to restore the confidence of the consumers, as well as optimized systems that provide their identification and information sharing shall be used [4]. Expansion of the rapid coordinated network, which provides data transfer between the airlines, airport authorities and security service personnel, ensures the law enforcement agencies to reduce the number of delays of air terminal communications and flights significantly. Nowadays, most air passengers suffer from this.

The recent accident is quite enough to imagine it. A man passed the explosives in his shoes, and that has not been identified by any control systems. The law enforcement agencies had to evacuate about 2-3 thousand people from the San Francisco terminal. If the terminal had adapted system, the monitoring cameras, X-ray facilities and wireless communications would identify the necessary person at the checking point, and would transfer the information to all the services of the airport and law enforcement agencies beyond it rapidly. Therefore, the suspects would be arrested, and the provocation would be avoided [6].

Nowadays, such systems are applied, since most of new technology components and its development are available. Nevertheless, the integration is of great importance, and the most difficult point is that, various personal communication protocols are used for the applications to provide security. Combination of available modern communication standards will provide to accelerate the integration of the applications, and ensure new opportunities for data transfer.

CONCLUSION

The article gives provisions to solve wide range of issues facing the national law enforcement system, state security system and defense authorities of the country with the use of biometric technologies. The factors providing the search and identification in the database of national criminalistics are defined. The ways of using biometric technology to ensure security are explained.

In conclusion, the following recommendations can be given:

- Integrated biometric information system should be available for the search and detection of

suspects. scenarios of the work of the law enforcement officials, which support the system, should be apparent;

- The identification process should be carried out close to real-time mode, and processing time of data entries should be minimal;
- Successful resolution of these issues at the state level is possible through the use of biometric information technologies;
- Developing distributed system for the collection and storage of multimedia data (pictures, video records, etc.);
- Interactive search of suspects from the databases, which include the data collected as the result of investigations and operational-searches;
- Biometric network system should be established and used to prevent undesirable phenomena in different situations (terrorism, crimes, etc.) and to provide security globally.

REFERENCES

- [1] V.V. Satyanrayanarayana Tallapragada and E.G. Rajan, Multilevel Network Security Based on Iris Biometric, 2010 International Conference on Advances in Computer Engineering Bangalore, India, 2010, pp. 908-912.
- [2] <http://igate.com.ua/lenta/2368-fbr-zapustilo-globalnuyu-sistemu-raspoznavaniya-lits>.
- [3] It is offered to apply technologies of recognition of persons to information protection (In Russian), Information Security journal, 29.10.2008. http://www.itsec.ru/newstext.php?news_id=51127#sthash.HQGrMBJh.dpuf.
- [4] <http://www.itsec.ru/articles2/Oborandteh/biometricheskie-tehnologii-vchera--segodnya--zavtra#sthash.FKdLyNn9.dpuf>
- [5] S.C.Mahmudova, Of the role the biometric network **In recognition of human**, "Electronic problems of state building," (In Azerbaijanian) the Republican scientific-practical conference on 4 December 2014, pp. 148- 151.
- [6] E.Jun Yoon and K,Young Yoo, A New, Biometric-based User Authentication Scheme without Using Password for Wireless Sensor Networks, IEEE 20th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Paris, France, 2011 27-June 29, pp. 279 - 284.

BIOGRAPHIES



T. Kazimov is a head of department at the Institute of Information Technologies. He has PhD on physically-mathematical sciences. He is author of more than 80 scientific articles. During recent years, he has been working on problems of development of information systems in "Euromat" computer networks, web-pages, national keyboard, automation of education process, sound recording of texts in Azerbaijani language through computers establishment of KIS of various appointments.



Sh. Mahmudova is a chief engineer of the project at the Institute of Information Technologies. She has PhD degree in technical sciences. She is the author of 70 articles. She was elected deputy editor-in-chief of IJIIP. Sh.J.Mahmudova was elected a reviewer of International Journal of Automation and Power Engineering (USA). Sh.J.Mahmudova was elected a reviewer of Journal of Control Engineering and Technology and British Journal of Applied Science & Technology.

At present, she the "Human face based on photo-portraits of methods and algorithms for the recognition of racial identity" is engaged in scientific research on the subject.