JOURNAL OF SCIENCE OF THE MILITARY ACADEMY OF LAND FORCES

Volume 49 Number 4(186) 2017

DOI: 10.5604/01.3001.0010.7226

POSSIBILITIES FOR THE USE OF BIOMETRIC DATA IN SECURITY SYSTEMS

Marian KOPCZEWSKI*
Tomasz SMAL**

* *Faculty of Security Sciences, General Tadeusz Kościuszko Military Academy of Land Forces*
e-mail:marian.kopczewski@awl.edu.pl

** *Faculty of Management, General Tadeusz Kościuszko Military Academy of Land Forces*
e-mail: tomasz.smal@awl.edu.pl

Received on 11th November; accepted after revision in May 2017

Summary:

Possibilities for the use of biometric data are growing and hence their practical application is also increasing. Therefore, an important element to be considered in the design, construction and exploitation of systems using biometrics is the question of identifying a specific person and assigning him or her to the relevant data contained in the documents or databases. The ability and, in some cases, the need to use biometric data results from the growing use of information technology in everyday life and the ever increasing attempts to steal the identity of those using these technologies. Modern IT systems often have a high level of security in terms of protection and access to data, and in particular the management of security systems. The article presents an outline of the theory related to the possibility of using and applying biometric data to provide security and have the ability to inspect officers of various departments. The subject of analysis also considered the possibility of using security measures in the form of biometric data identification for the purpose of securing the security services.

Keywords:

biometrics, management, security, services

INTRODUCTION

Biometrics is a branch of science that deals with the establishment and confirmation of identity based on the measurable characteristics of the body. Biometrics is also a col-

lection of methods and techniques of verifying and confirming the identity of individuals based on their biophysical and behavioral traits [5]. According to another source, biometrics is considered to be a set of techniques of measuring the physical and behavioral characteristics of a human being in order to automatically recognize a given person or to confirm or reject his or her identity for security purposes [2].

Biometrics can also be defined as a method of automatic personal identification based on certain physical or behavioral characteristics of a human being. These features constitute biometric data. The greatest development of biometric systems began in the 90s of the last century [12]. At that time, the works started on improving, especially in the area of security, among others, the protection from fraud by unauthorized persons.

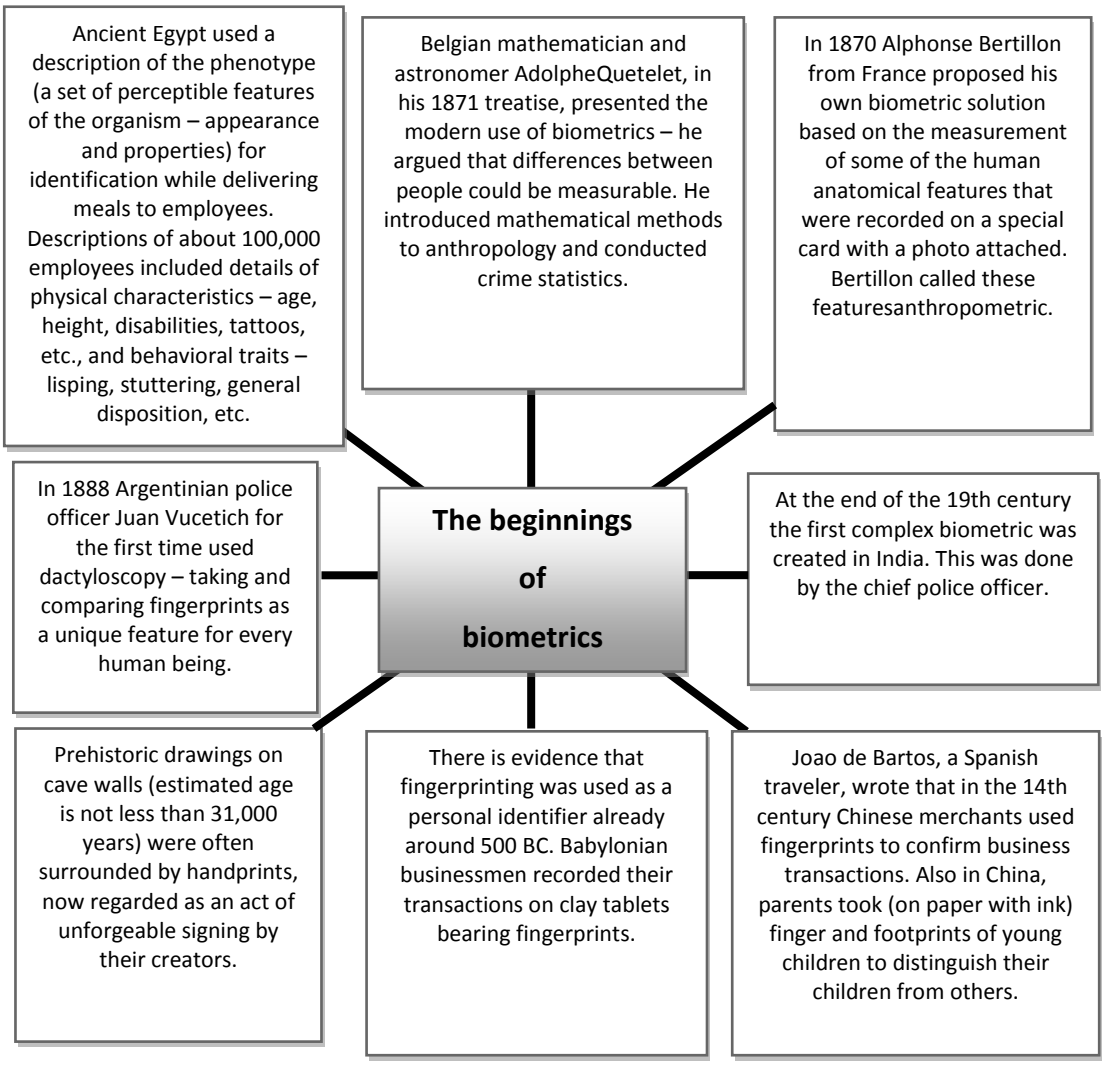

Fig. 1. Using biometrics over the known history of mankind

Source: Biometria [in:] Patrol – Magazyn Securitas w Polsce No. 4, Warszawa 2007, p. 6

The term “biometrics” comes from the Greek word “bio” (life, alive, life processes) and “metrics” (measure). Biometrics deals with the measurement of biological traits and its main function is the automatic recognition of individuals. The idea of using unique body features for identification has been known for hundreds, or even thousands of

years [4]. The Babylonians used a fingerprint in wax as a seal. The development of integrated biometric systems is, however, a very young scientific discipline dealing with the application of mathematical and statistical methods in solving biological problems and especially in the planning and analyzing experiments. The first mention of it comes from the 1930s. English naturalist Francis Galton (1822-1911) is considered to be the "godfather" of biometrics, as he recognized biometrics as a promising new direction in science [15].

Due to the high accuracy and reliability of devices measuring biometric data and the high computing power of computers capable of analyzing these data, biometric has become a popular way of protecting access to data from unauthorized person. Figure 1 shows the noted examples that can be considered to be the beginnings of using biometrics over the known history of mankind [4].

1. THE ESSENCE OF BIOMETRICS

Contrary to some ideas and assumptions, biometrics is not a branch of metrology dealing with measuring the parameters and characteristics of various biological systems. Such measurements and observations are indeed made on the basis of anatomy, histology, anthropology, physiology and biophysics, but the very process and methodology of appropriate measurements do not differ in any conventional way from measurements used in technology, physics or chemistry.

However, such duplicated observations and measurements, accompanied by factors that reduce their credibility, constitute a very uncertain and inconvenient ground for attempting to conclude properties of objects and phenomena on their basis, as well as for attempting to make generalizations and practical applications of research results. Therefore, statistically elaborated results are an essential element of every measurement and assessment regarding biological systems. Due to such elaboration, it is possible to bring many unreadable measurements to several easily interpreted indicators. In addition, skillfully applied statistics provide the possibility of precise inference based on a large number of difficult interpretations of data. In this way, biometrics is a tool extracting order from chaos, a factor allowing to overcome the fundamental contradiction that exists between the nature of personally individualized biological observations and the tendencies originating from science to formulate general and universal judgments [16].

Enthusiasts of biometrics consider it to be the safest and most convenient tool for authorizing and identifying a given person, while at the same time preventing unauthorized access to sensitive and non-public information. Opponents of biometrics, on the other hand, point to the possibility of violating human rights and the fact that in the age of new technology biometric data are easily falsified. In their opinion, doubts about the possibility of human rights and freedom violation are due to the widespread use of this type of data as well as the commonness and lack of control over their collection and processing.

Two main sections of biometrics are distinguished, i.e. static – physical-biological and dynamic – behavioral (Figure 2). Static biometrics consists of recognizing features of

human body such as facial geometry, retina and iris, voice, hand and finger geometry as well as fingerprints. Dynamic biometrics, in turn, recognizes such behavioral traits as way of walking, way of pressing the keys, signature features or signing.

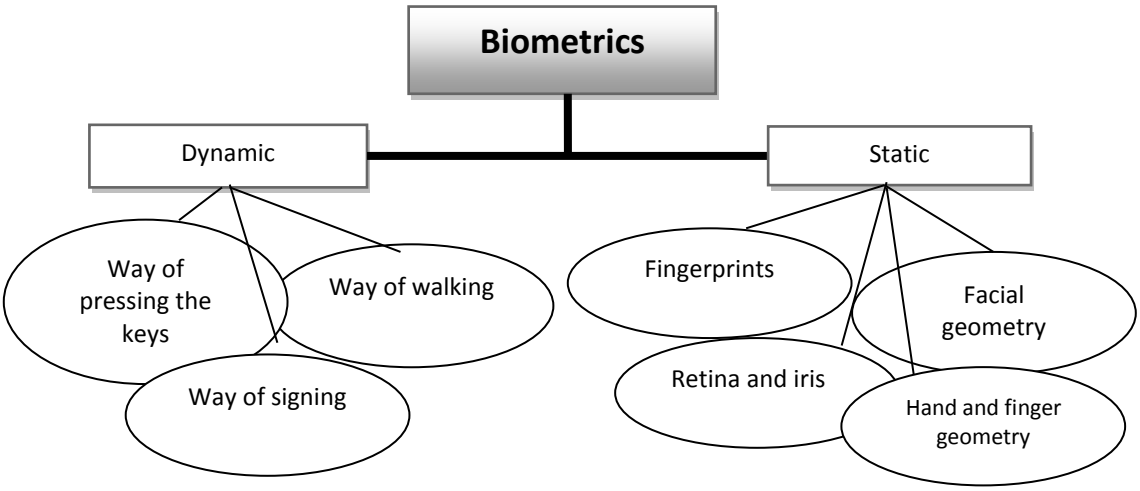

Fig. 2. Basic sections of biometrics

Source: M. Chałon: Ochrona i bezpieczeństwo danych oraz tendencje rozwojowe baz danych. Wrocław 2007, p. 40

Currently biometrics can provide a set of complex tools that are largely intended for the detailed identification and verification of people's identities. This process is carried out by means of multi-segment analysis of varied and unique physical or behavioral traits. It is worth to explain the essence of the concepts of verification and identification. Verification is based on a detailed check whether or not a person identifying with a given identity is actually the one with whom he or she identifies. The verification process is thus a task possible to implement with the use of relatively inefficient IT systems. The whole process consists in the comparison of a sample recorded by a special device, e.g. a reader, microphone or camera, with a template stored in the database. However, as far as identification is concerned, the process is more complex, because it often happens that the identification of a given person is based on a very large range of data. The data collected by a reader must then be compared to the databases of millions of people. Identification is mainly used by government institutions, security services (e.g. police), the judiciary and the military.

In practice, various methods of identification and verification of persons are used. All these methods, however, are different primarily in terms of effectiveness, costs and the so-called invasiveness. Invasiveness, nonetheless, is an element of substantial subjectivity; in the case of identification and verification it mostly concerns the violation of personal space and dignity, rather than the intrusion of special measuring devices into the human body.

2. LEGAL ASPECTS OF BIOMETRICS

The application of methods and techniques of biometric verification and identification becomes more and more common in many areas of life and the economy. However, despite the fact that biometrics is used in everyday practice, not all the issues associ-

ated with it are clearly established. It is very important to meet the highest security standards for data collection and storage. Biometrics specialists point out that the priority here is the security of individually collected identity traits in an advanced ICT system, where the widespread use of electronic services is taking place through more and more modern devices. It is of particular importance that the development of technology should be followed by understanding and interpretation of the law. Currently, there is a lot of debate in the public sphere regarding the personal data protection and the understanding of certain legal aspects of using biometrics.

According to the Personal Protection Act of 1997 (UODO), personal data is "any information related to an identified or identifiable natural person" [7]. Due to the fact that biometric data in principle fulfills the conditions provided for in the definition, in most cases the aforementioned Act and special laws will regulate its legal status [11].

Biometric data is not explicitly defined in UODO, but if it corresponds to the condition set out in Art. 6 of UODO (related to an identified or identifiable natural person, taking into account Art. 6 (2-3)), it shall be protected under this legal act. The lack of legal definition in UODO does not mean that there is no such definition in the Polish or EU legislation. The concept of biometric data appears in the Act on passport documents [8]. It was defined in it as a facial image and fingerprints placed in passport documents in an electronic form (Art. 2 (1)). The drafting of the passport document, in accordance with this Act, is the transfer of personal and biometric data of the person applying for a passport document into a passport book in a graphic and electronic form (Art. 2(4)). It seems that the definition presented in the Passport Documents Act is quite narrow, as in the literature personal data includes DNA, iris image, etc. [1].

In the EU law, the issues related to biometric data are regulated by the Council Regulation (EC) No 2252/2004 of December 13, 2004 on standards for security features and biometrics in passports and travel documents issued by the Member States, under which a facial image and fingerprints are considered to be biometric data (Art. 2 (2)) [9].

The Personal Data Protection Act lists the genetic code, among others, as sensitive data. This means that biometric data should be treated as sensitive data, so that at least an increased level of data protection should be used for processing such data.

With regard to the collection of biometric data in the form of fingerprints and their inclusion in the database in order to identify access and record the working time in an enterprise, it seems appropriate to refer to legal provisions in two cases [11]:

- an employer will use biometric data in work time registers, however, the biometric data will be stored securely only on contactless cards and compared by a secure biometric reader rather than the central software – an employee accepts the solution;
- an employer will use biometrics only to control access to rooms in company buildings (data on the server).

The reference of the UODO to the Labor Code and the related possibility and legitimacy of consent to the collection and storage of biometric data is essential in terms of using biometric technology in business organizations.

The Labor Code defines requirements for the collection of biometric data [3]. It explicitly sanctions that the voluntary placement of biometric data in the form of a biometric pattern on a card means that data is at the disposal of the holder. In this case, the employer cannot use this kind of data, and any attempt to use biometrics involves the disproportionate amount of resources and efforts that must be incurred in creating a secure data storage system.

However, the Labor Code standards in relation to the work regulations provide great opportunities to use biometric solutions to measure working time or access to office spaces. In the Labor Code it is clearly stated that in specific cases the work regulations may establish "work organizations, conditions of staying at the workplace" as well as "adopted by a given employer method of confirming the employees' arrival and presence at work". As "the employer may require other personal data than specified in § 1 and 2, if the obligation to provide it results from separate provisions", and Art. 104 introduces, under certain conditions, the requirement for the existence of the work regulations, the consent to biometric measurement of working time or access to office spaces could be legalized by the Legal Code rules [11].

3. BIOMETRIC SYSTEMS AND THEIR FUNCTIONING

On the grounds of the statistical data it can be stated that most often incorrect functioning of the system is related to a human error, so the improvement of existing systems and designing the new ones is aimed at, among others, eliminating such errors. Based on the available studies it can be also said that systems using biometrics give greater warranty for the proper identification of a system user. These systems are associated primarily with taking fingerprints or scanning the iris. In the meantime, new physical and behavioral features of human, unique to him/her and thus differentiating him/her from every other person, are constantly sought. Some of them are already available on the market as ready solutions, while others are in the research and testing phase.

An important element that enhances the chances of designing and introducing a biometric system is the acceptance of measurement and the way of "taking" a given biometric characteristic. Registration and implementation modules work together and carry out tasks related to the collection of raw biometric data, extraction of traits, comparison of sets of traits and decision-making. Figure 3 shows the scheme of action for processing biometric data.

Another issue concerns devices and ways of controlling biometrics, all kinds of readers and control gates. They should be easy and quick to use, precise in operation (error level in rejecting and accepting), resistant to inference attempts and of course not too expensive at the purchase and use stage. For devices that are intended for remote or local authorization, it may be necessary to recognize not only the person but also his or her will. This may cause a situation where devices will need to have the ability to rec-

ognize actions that reflect the will of a given person. In such cases, for example, the person's signature – specific hand movements, eye movements or other parts of the body, as well as a spoken word or sentence, can be used.

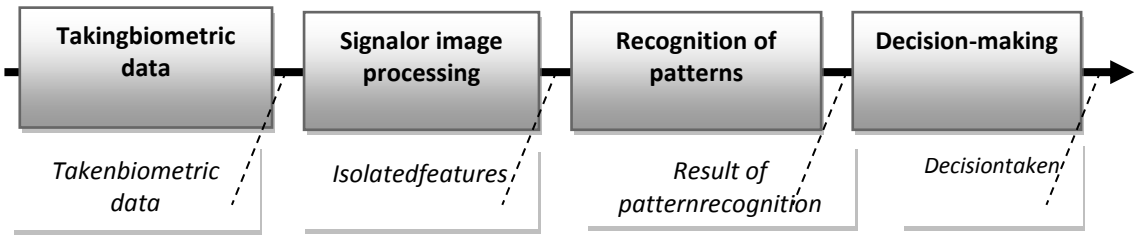

Fig. 3. Stages of processing biometric data

Source: J. Barta, P. Fajgielski, R. Markiewicz: Ochrona danych osobowych. Komentarz.Kraków 2007, p. 342

At present, there is a wide range of biometric systems on the biometric device market. The most popular of these are fingerprint reader devices used mainly for access control systems and the so-called terminals based on digital fingerprint verification, which also operate in the form of a dual system, allowing for two types of authorization through fingerprints and proximity cards. The work of biometric systems performing verification functions is based on confirming the identity of a person who is submitted to the process. Practically, this means initiating authentication through proper preselection of verifiable data, for example, by using biometric data stored on a carrier, which can be a card. A proper vector of biometric traits is compared with its equivalent in the system and a decision is made whether or not they are compliant. This mode is called 1:1 mode. This solution allows verification in systems with significantly lower performance requirements, and also requires less time to complete this function.

Identification systems are designed to explicitly determine a user's identity. They do not confirm the biometric characteristics of a given person but, given his or her biometric traits, they can clearly identify that person. After reading the biometric features and converting them digitally, they search the available data to find the closets object to the one examined. This is the basis for determining the identity of anexamined person. Taking into account how these functions work, identification is defined as 1:N mode (one to many). The statement "closest to the examined one" says that a positive answer is possible after reaching a certain threshold of compliance between the sought set of biometric traits with the one found.

The operation of biometric systems should prevent re-registration of a user in the database. In other words, the system should not allow for the registration of the same identity with other identification data. This is particularly important in high security systems and such are being used in emergency service organizations. The change of personal data does not affect the identification result, and a person once entered in the database (as a specific set of biometric data) is always identified under the originally entered data. The result of this approach is effective protection against attempts to hide or change identity.

4. THE USE OF BIOMETRIC TECHNOLOGY

Physical characteristics that can be used in biometric systems include: timbre, smell, fingerprint (print of the finger and fingertip), finger blood vessels, hand geometry, face geometry and facial features, face temperature distribution, analysis of facial surface structure – skin, ear geometry, mouth geometry, iris characteristics, retina characteristics, wrist vein pattern, hair and nail structure, EEG, ECG and DNA identification. Considering the behavioral features, the characteristics of voice, speech, mouth movement, eye movement can be listed. Writing (handwriting), typing method, gait characteristics belong to other traits that can be distinguished [30].

Some of the abovementioned features are already in use, some are in testing and implementing phases. Not all of these features have practical applications. There are also new proposals that meet the characteristics described below and may be used in the future as biometric features. They include: the shape of the whole human body, analysis of facial or head vibrations during speaking, study of the internal body structure and its vital functions, analysis of magnetic or electrical fields generated by the human body or reactions to such fields. The percentage of used individual biometric features is shown in Figure 5.

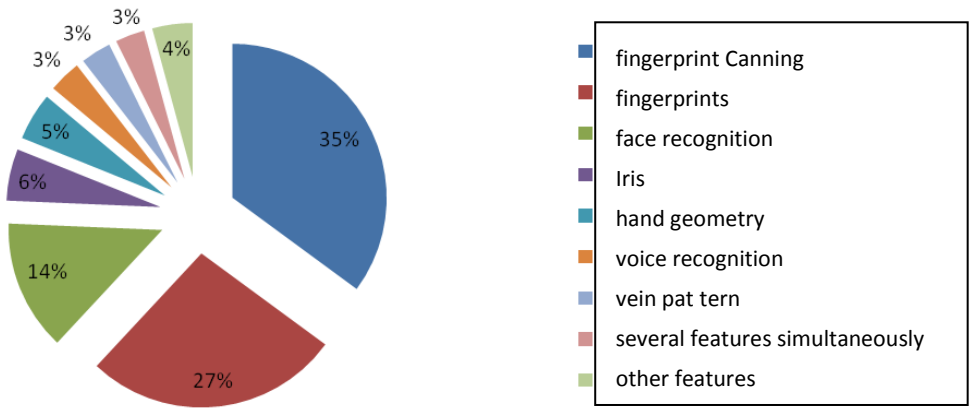

Fig. 5. Percentage of used individual biometric features

Source: I. Iskierka, S. Iskierka: Przegląd podstawowych technologii biometrycznych. Częstochowa 2010, p.116

Main areas of application of biometrics can be classified as follows [11]:

- justice and defense: identification of corpses, criminal investigations, identification of terrorists, search for the missing, military and special institutions, strategic institutions - banks, power plants, refineries, rescue and security services;
- public administration: ID cards, driving licenses, digital signature, social benefits, passport control, border control;
- commercial application: computer work, data protection, e-commerce, Internet access, credit and payment cards, physical access control, mobile

phones, medical records management, e-learning, working time management, library and public data access, mass events.

When analyzing security measures using biometric data, it should be stated that they have very high prospects for future use. What distinguishes biometric data from other forms of identification and verification, i.e. the impossibility of losing, forgetting and falsifying them, as is the case with any passwords, keys, etc., gives them the value of timeless protection. However, despite the unquestioned usefulness of biometric technology in various types of security, the essential question arises of which of the currently available forms is the best.

5. DATA SAFETY

Assuming that the security of identification data in information systems is on a sufficiently high level, the main problem faced is the issue of assigning a person to a document that is used to identify that person. This is the purpose of the use of biometric data that is placed in the identification document. Such data can be of two kinds. On the one hand, this data can be verified directly – without the use of specialized equipment, for example, biometric photo; on the other hand, this is the data recorded in the electronic part of the document – in a microprocessor, which can only be verified using specialized devices, i.e. fingerprint readers.

The analysis of main biometric technologies clearly shows that every biometric system is exposed to different threats. Therefore, each system requires different protection. It is worth mentioning that the communication channels within individual biometric technologies are an essential part of the whole system. Thus, it is important to provide them with sufficient protection. This is significant because securing communication channels inside a single device analyzing biometric data is a much easier step in the process, and what is more, it can be used to secure the entire system.

Any attempt to break the biometric system can focus on a wide range of different links throughout the whole biometric system. Significant number of attacks and attempts to break the system is very similar to attacks on freely chosen information systems. An example can be an attack attempt at the data processing stage, which indicates the replacement of the main system algorithms. This can be done by direct interference in equipment or software. Therefore, principles for physical, anti-theft and anti-virus protection known from other departments creating information systems remain important. Thus, good practices that are obligatory for designing any securing information systems should be used for all components of the biometric security system [6].

The spectrum of threats to biometric systems, due to their specificity, is slightly broader than in the case of standard information systems. Figure 6 shows the main types of biometric systems threats.

Another important fact is that, as with other security systems, a user of the biometric security system is its integral part. Therefore, the user of such a system should be adequately trained for using a particular system and possible abuses. It is well known that the entirety of the system as stable and strong as its weakest link.

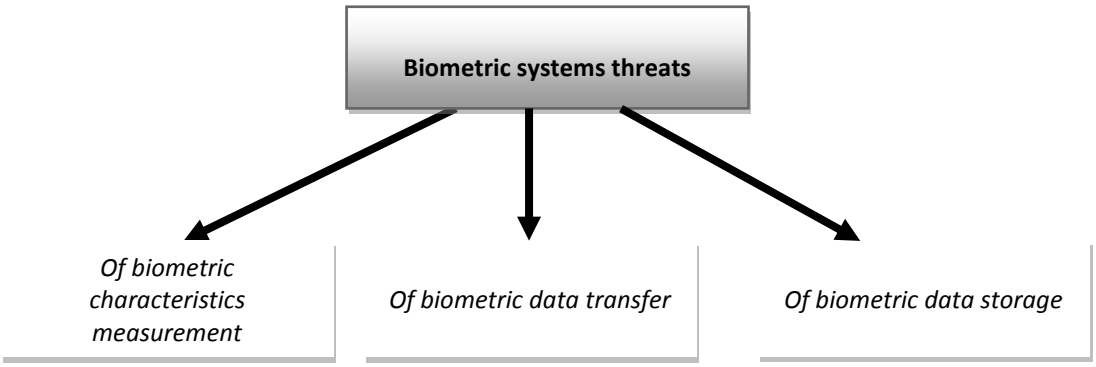

Fig 6. Basic threats to biometric systems

Source: Ł. Stasiak, A. Czajka, P. Strzelczyk, M. Chochowski, A. Pacut: Od biometrii do bezpiecznej biometrii, Warszawa 2007, p. 5

CONCLUSION

Summing up the theoretical biometric solutions presented in this paper, the conclusion can be drawn that biometrics is one of the safest and most convenient tools for authorization and identification of individuals, while preventing unauthorized access to information, secrets and data by persons negatively identified. Biometric systems are associated primarily with taking fingerprints and iris scanning. Nevertheless, new physical and behavioral traits of human, unique to them and thus differentiating them from every other person, are constantly sought. Some of them are already available as ready solutions on the market, others are in the research and testing phase. When analyzing security measures using biometric data, it should be stated that they have very high prospects for future use. What distinguishes biometric data from other forms of identification and verification is the impossibility of losing, forgetting and falsifying them, as is the case with any passwords, keys, etc.

The article has discussed main issues related to the prospect of using and applying biometric data. The conducted analyses make it possible to conclude that biometric systems are quite well known security systems, which provide a high level of security and facilitate the identification process. On the other hand, these techniques are still considered to be high-cost techniques that lead to data abuse.

REFERENCES

1. Adamski A. et all., *Internet. Ochrona wolności, własności i bezpieczeństwa*. Warszawa 2011.
2. Anderson R., *Inżynieria zabezpieczeń*, Warszawa 2007.
3. Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*. Kraków 2007.
4. Biometria [in:] "Patrol" - Magazyn Securitas w Polsce nr 4, Warszawa 2007.

5. Chałon M., *Ochrona i bezpieczeństwo danych oraz tendencje rozwojowe baz danych,* Wrocław 2007.
6. Denning D., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
7. Dz. U. z 1997 r. Nr 133, poz. 883 ze zm.
8. Dz. U. z 2006 r. Nr 143, poz. 1027 ze zm.
9. Dz. Urz. z 29 grudnia 2004 r., UE L 385.
10. Iskierka I., Iskierka S., *Przegląd podstawowych technologii biometrycznych*, Częstochowa 2010.
11. Kaszubski R. W., *Biometria w bankowości i administracji publicznej* Warszawa 2010.
12. Niedziejko P., Krysowaty I., *Biometria. Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie* [in:] "Zabezpieczenia" no. 4, Warszawa 2006.
13. Pieprzyk J., Hardjono T., Seberry J., *Teoria bezpieczeństwa systemów komputerowych*, Gliwice 2005.
14. Stasiak Ł., Czajka A., Strzelczyk P., Chochowski M., Pacut A., *Od biometrii do bezpiecznej biometrii*, Warszawa 2007.
15. Ślot K. *Wybrane zagadnienia biometrii*, WKiŁ, Warszawa 2008.
16. Tadeusiewicz R., Izworski A., Majewski J., *Biometria*, Kraków 1993.

BIOGRAPHICAL NOTE

KOPCZEWSKI Marian – Professor DSc. hab. Eng. worked on high command and didactic positions, finishing his military career at the rank of colonel as the department head – professor at WSOWOPL in Koszalin. Since 1997 he has been a research and didactic worker, has popularized modern teaching methods and led the process of dissertation in the field of Security, Crisis Management, Geography of Security as well as IT and European Studies. In his scientific work, he focuses on the analysis and evaluation of the possibility of using information systems in management and teaching as well as national and internal security systems, including European and Euro-Atlantic political and military integration. He is the author and co-author of more than 500 different national and foreign publications, including several monographs thematically related to national security. He directs national and foreign scientific research works and has supervised 6 PhD students. He is a member of the Editorial Board of Journals of Science of the Military Academy of Land Forces and the Chairman of the Scientific Committee for Journals of Science Education for Safety, the Polish Association for Security Science and the Polish Association for Defense Science, the president of the Polish Association for Production Management and the Polish Association of Creative Teachers.

SMAL Tomasz – Col. DSc. Associate Professor graduate of the Military Academy of Technology and the University of Defense in the Czech Republic. He conducts scientific activities in the fields of: the operation of armaments systems, military logistic support, technical and transport security, and IT support for military and crisis operations. He

has completed 14 research projects. He is the author or co - author of about 130 articles and 8 publications; the most important ones are listed in journals indexed on the ISI Web of Science and SCOPUS. He was awarded numerous times for scientific andmilitary activities. He is a member of the Editorial Board of the 'Journals of Science of the Military Academy of Land Forces', the Scientific Board of 'PWSZ Journal of Science' in Włocławek of 'Economics and Management' series and the Program Board of the OBRUM Journal 'High Speed Track Vehicles'. He is also a member of the Combat Service Support Group of the NATO Standardization Agency, the Polish Logistic Association, the Polish Association for Security Sciences and the Polish Association for Defense Sciences.

HOW TO CITE THIS PAPER

Kopczewski M., Smal T., (2017) –Possibilities for the use of biometric data in security systems. *Zeszyty Naukowe Wyższa Szkoła Oficerska Wojsk Lądowych im.gen. Tadeusza Kościuszki Journal of Science of the gen. Tadeusz Kosciuszko Military Academy of Land Forces*, 49 (4), p. 168-179, DOI: 10.5604/01.3001.0010.7226