BIOMETRIC SYSTEMS IN AIR TRANSPORT

Luboš SOCHA[1] – Peter HORŇÁK [2]- Vladimír SOCHA[3] - Anna ČEKANOVÁ[4] - Peter HANÁK[5]

Abstract: *The article deals with the issue of obtaining biometric data to identify individuals who may pose a risk and potential threat to air transport. It characterizes individual methods of obtaining biometric data, using biometric systems, evaluates their advantages and disadvantages. At the same time, based on a questionnaire survey, it analyzes and assesses passengers' attitudes towards the use of biometric data within security screening in a passenger handling process.*

Key Words: *biometric system, security, terrorism, air transport*

1 INTRODUCTION

Aviation safety is inherently associated with the high professionalism of airline specialists and the reliability of aviation systems and technologies. It is devided into Safety, which is designed to ensure operational safety and Security, which primarily focuses on eliminating possible risks associated with unlawful acts. The main task and mission of security is checking persons and goods to ensure flight safety. [1] Terrorist attacks on the World Trade Center on September 1, 2001, in which 3,404 people were killed and about 6,000 people injured, defined a new threat to air transport, termed "terrorism." [2] [3]. Immediately after these events, where civilian aircraft were used as weapons, negotiations were initiated, in particular, between the US and Europe on enhancing aviation safety. With regard to possible threats to countries by terrorist attacks, a number of security measures have begun. One of them was the mass introduction of biometric systems to identify and monitor the movement of individuals to eliminate these threats. Large databases with biometric data of individual travelers, persons suspected of interfering with terrorist organizations or persons who could be a potential threat began to be created. Systems also use access to databases of various security agencies that already have their extensive databases of risk persons. Databases were made mainly by fingerprints and photographs, and are now expanding with additional biometric data. At present, large world airports are equipped with the most advanced systems for verifying, checking and identifying passengers. These are the most diverse systems that can identify passengers individually or identify a suspect or risky person in a crowd at an airport. Fingerprints, face recognition systems, thermovision, eye iris scanners, eye retina scanners, voice recognition software, hand geometry are used to identify people. In cases where a person cannot be identified and there is a high suspicion, it is possible for a person to detain and take DNA samples and compare them to international databases of different security agencies, or the person is not registered.

2 TYPES OF BIOMETRIC SYSTEMS IN AIR TRANSPORT

Biometric systems used in air transport can be divided into two groups, namely systems used to identify, authorize and verify aerodrome staff and systems used to identify and authenticate people, or passengers.

2.1 Fingerprinting

The fingerprint identification method is historically the most widely known, most widely used and most widely published biometric method. This method is followed by all other modern methods such as hand geometry, hand veins, handprints, and the like. For the past century, fingerprints have been used to identify, especially for its properties of uniqueness and durability over time. With the

[1] Ing.,PhD.,PhD, LF TUKE, Rampová 7, Košice, tel.: +421556026199, e-mail: lubos.socha@tuke.sk
[2] Ing., LF TUKE, Rampová 7, Košice, tel.:+421911293181, e-mail: peter.hor.nak@gmail.com
[3] Ing.,Bc.,Ph.D., FD CVUT, Horská 3, Praha, tel.: +421948205335, e-mail: ing.vladimir.socha@gmail.com
[4] PhDr., PhD., LF TUKE, Rampová 7, Košice, tel.: +421556026164, e-mail: anna.cekanova@tuke.sk
[5] Ing., PhD., LF TUKE, Rampová 7, Košice, tel.: +421556026200, e-mail: peter.hanak@tuke.sk

development of computer technology, this identification method has to become automated to secure its place even today. Fingerprint identification is especially preferred for the relative ease of obtaining a comparison sample for a very high percentage of the population. (It is not possible to identify only people who have lost both hands and feet, but this is only very unlikely. [4]

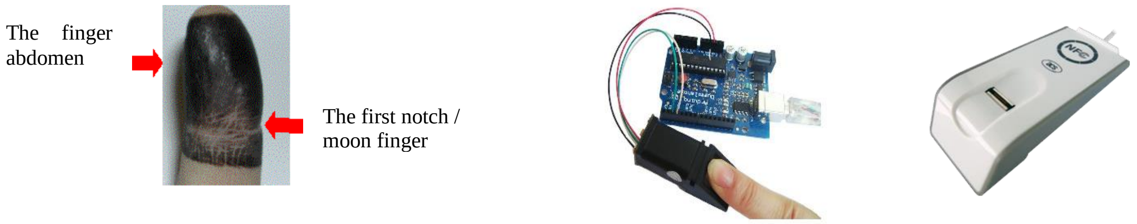

Figure 1 Methods of fingerprint capture. Imprints obtained with ink and paper [3], sensor for static fingerprint scanning [5] and template fingerprint readers [6]

Advantages:

- Very high accuracy
- It is the most economical biometric identity verification
- It is the most developed way of biometrics
- Easy to use
- Requires little storage for biometric templates, reducing database size (less memory usage)
- It is a standardized way

Disadvantages:

- It is still very disturbing for some people, because it is associated with the identification of criminals
- It may be a mistake in dry or dirty hands, and it is also not very appropriate for children because the size of their prints is changing rapidly
- Fingerprint captured as a 500 dpi image (8 bits per pixel resolution) such finger image requires a relatively large memory space of approximately 240 Kbytes, so compression is required [9]

2.1 Hand geometry

The hand geometry recognition system is one of the oldest implemented methods. For this method, it is very important that the shape of the hand does not change from a certain age. This method works on two or three dimensional measurements of the length and width of individual fingers, joints, and bones. The measurement process does not affect nail length, dirt, sweat, and even minor surface skin injuries. Identification can only make it impossible for more extensive hand injuries, such as finger fractures or amputation. [3] [4]

Hand geometry recognition devices use a simple measurement principle and a 3-dimensional length, width, thickness, and hand surface of a particular person placed on a five-position pad with a CCD camera.

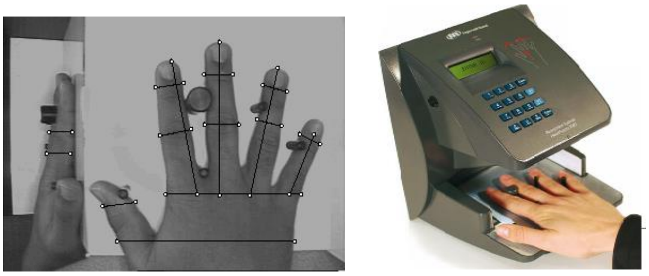

Figure 2 Procedure in hand geometry recognizing [7] [8]

Advantages:

- It requires special hardware to use, but is very easy to integrate into other devices or systems
- This way has no public attitude problems because it is most often associated with authorized approach
- The amount of data needed to uniquely identify a person is by far the smallest

Disadvantages:

- The device is financially demanding
- A large number of devices
- A problem with people with certain illnesses (e.g. arthritis - where may be a problem to correctly place a hand on the scanner) [9]

2.3Voice verification

For decades, criminals have been using voice samples to compare. In civil practice, however, this technology is slowly starting to push forward. The shape of the teeth, mouth, vocal cords and tongue makes the voice of different people quite different. The pre-stored digital voice samples serve to verify the subject's identity - these are key phrases or words spoken. The advantage of verifying identity using voice lies not only in the uniqueness of the human voice but also in the flexibility of key sentences. [3]

Voice recognition, i.e. voice recognition among others in the real world, is much more challenging and there is currently not a sufficiently accurate system. [10]

Advantages:

- Not intrusive way
- Validation time is about 5 seconds
- Cheap technology
- Low hardware performance

Disadvantages:

- Low accuracy
- A person's voice can be easily recorded and used for unauthorized entry
- Disease, rhinitis, and the like can change the voice of a person, and so authentication can become impossible. [9]

2.4 Signature verification

This method dates back to 1977 and uses the uniqueness of the combination of anatomical and behavioral attributes of man that manifest when they are signed. Dynamic signature devices are often mistaken for terms like electronic signature (encrypted key) or signature - image capture devices. From the manual signature, it is possible to electronically detect the movement, shape and pressure in writing, which can be used to verify a person. Most of these devices use dynamic signature properties, although there are combinations with static and geometric signature properties. The basic dynamic properties are speed, acceleration, timing, pressure and tensile direction recorded in the three-dimensional coordinate system. Axes "x" and "y" serve to determine the stroke speed and direction, the coordinate "z" determines the pressure on the washer. (See Figure 3) Unlike the static signature image that can be taught and imitated, it is impossible to learn the dynamics of the signature just from the picture.

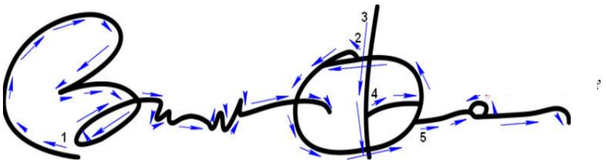

Figure 3 Dynamic recognition of a signature[11]

Advantages:

- Not intrusive way, people are accustomed to signing
- Short validation time (approx. 5 seconds)
- Relatively cheap technology

Disadvantages:

- Signature verification is designed to allow the person to be verified on the basis of his/her unique signature. The problem is that individuals who are unable to sign exactly the same way may have a problem verifying the signature
- Error rate = 1 out of 50 [9]

2.5 Retinal scanning

The image of the vessel's structure on the background of the human eye in the vicinity of the blind spot is used for recognizing the person according to his/her eye retina. The retina is a light-sensitive surface on the back of the eye and is composed of a large number of nerve cells. To obtain the image, a low-intensity light source and an optical-electrical system are used. At present only one infrared LED is used, which reduces the risk of dangerous eye irradiation comparing to a system where several LEDs were used. Retinal Verification is a very accurate method of identification. Its use requires a user to look into a precisely defined area, which may be unpleasant for some people, and sometimes impossible, problematic, especially for people who wear glasses. It is mainly used in areas where it is necessary to ensure the highest degree of security. [4]

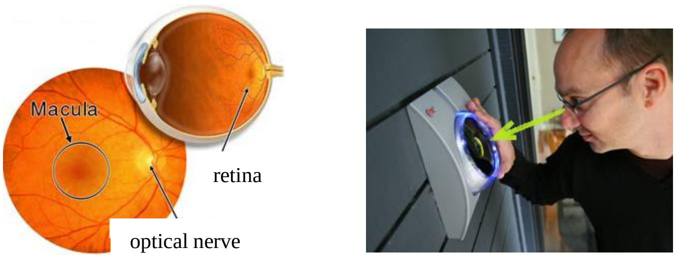

Figure 4 The retina and a retinal scanner [12]

Advantages:

- Very high accuracy
- There is no method to replicate the retina
- The dead man's eye gets worse very quickly so it cannot be used at all, so no further action may be taken, and by scanning one´s retina, make sure the user is living and authorized.

Disadvantages:

- A very disturbing way
- It sensors an eye retina and people think it's dangerous for their eye
- Scanning with a template can take 10 seconds depending on the size of the database
- Very expensive to set up [14]

2.6 Iris scanning

Automatic biometric systems for recognition of human eye retina are relatively newly developed. The first patent was filed in 1994 and developed by the US Nuclear Safety Office headed by Dr. John Daugman. The iris is the muscle inside the eye that regulates the size of the lens (i.e. the focus of the eye) based on the light intensity on the eye. Although the iris color and structure are genetically dependent, its sampling is not. The iris develops during the prenatal growth of the fetus and its sampling is random, so unique to every person, even twins, even one person has each iris different, and that makes these systems the most accurate of all. [4]

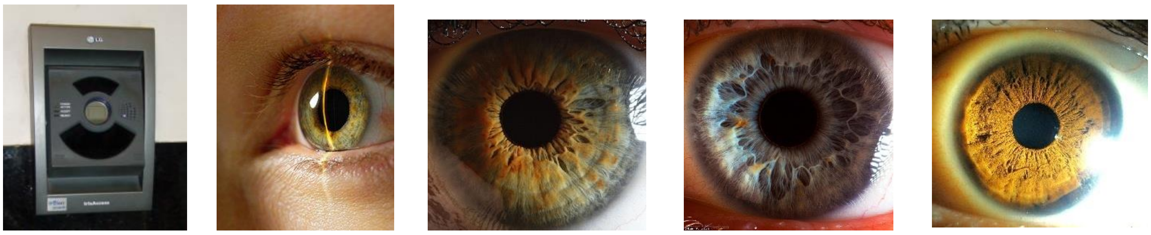

Figure 5 The Scanner, scanning the iris and variety of eye irises [15]

In the verification process, the applicant's map of the iris is compared with the benchmark test of statistical independence. If only less than one third of the data is different, the statistical independence test has failed, which means that the samples are not of the same iris.

Advantages:

- Very high accuracy
- The verification time is usually less than 5 seconds
- The dead man's eye gets worse very quickly so it cannot be used at all, so no further action may be taken, and by scanning one´s retina, you make sure the user is living and authorized.

Disadvantages:

- Disturbing, very annoying way
- Large storage space is required for the data to be stored
- Very expensive to set up [9]

2.7 Biometric passport

Following the events of September 11, 2001, the US began to push all its partners, especially those with whom they had visa-free travel, to include biometric identifiers in travel documents. It was about making biometric identifiers stored in travel documents, such as digital photography, fingerprinting, or a pattern of iris or retina that can clearly identify the person.

In May 2003, the ICAO International Civil Aviation Organization adopted a basic agreement on the inclusion of biometric identification in passports and other machine readable travel documents (MRTDs). Face identifier was selected as the global interoperable biometric data for assisted instrument identity confirmation.

In November 2003, the EU Council agreed on the objective of including biometric data on visas and residence permits issued by EU members to third-country nationals.

On 18 February 2004, the Commission adopted a proposal for a "Regulation Harmonizing Security Standards", including biometrics in the passports of EU citizens. In December 2004, after approval by the European Parliament, the "EU Passport Regulation" was adopted by the EU Council. On the basis of the wording of this regulation, passports must include digital face photographs and fingerprints. Passports must also be "machine-readable", they must contain a barcode on which computers will be able to search for personal information. [16]

The obligation to introduce travel documents with machine-readable data and so- An RFID chip that activates radio waves-based electronic readers containing the holder's biometric data has begun to apply to all EU Member States since 2006. These biometric data should be kept on a chip in travel documents but also in the European database called “The Schengen Information System II "(SIS II). The Slovak Republic joined the system on 9 April 2013. There was also the predecessor of the SIS, which was begun in 1988, the Slovak Republic joined it on September 1, 2007 and 28 countries are currently connected to the system. For the sake of further development and streamlining, the second generation of SIS has been built. There also exits the Visa Information System (VIS), which gathers biometric data for visa applicants and residence permitions to stay in EU countries.

In Slovakia, EU passports were issued from 1 April 2005 to 14 January 2008. From 15 January 2008, new passports with biometrics have begun to be issued with the first biometric data resembling a face and, from 22 June 2009, a fingerprint finger. [17]

These passports currently include:

- A digital photo chip
- Digital signature
- Fingerprint
- Demographic data from the last page of your passport

Figure 6 Biometric Passport Reader and RFID Chip in a Passport [18]

2.8 Facial recognition

Verification, that is, face recognition, is currently the most researched method, because face-to-face identification is very extensive and highly desirable, especially in terms of recognizing people in the crowd. Recognition is based on comparing the image from the camera to the image stored in the central database. To uniquely identify, most of the face shape and position of optically significant facets such as eyes, nose, mouth or eyebrows are used. The exact position of the eyes, the nose and the pier is not preserved, but only the distance of the eyes, the distance of the nose from the nose, the angle between the tip of the nose and one eye, and the like. This system has good results in laboratory tests, but in practice it is no longer successful. [4]

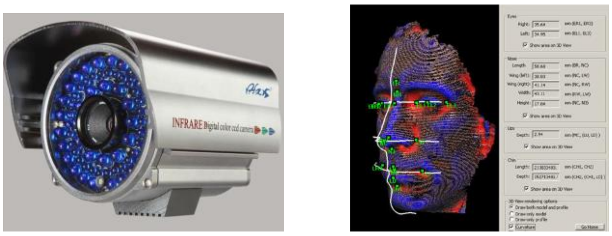

Figure 7 CCD digital high resolution camer and face recognition software [19]

In terms of practical use, the attractiveness of face recognition is understandable, but it is important to be realistic about the prospect of this technology. So far, face recognition systems have not been successful in practical applications.

There are two different approaches to recognizing face geometry:

- Geometric (based on facial features)
- Photoelectric (based on a facial image)

Advantages:

- Non-volatile technology - no physical contact is required
- Relatively inexpensive technologies

Disadvantages:

- 2D recognition is influenced by changes in lighting, the hair of the person, the age, and also when the person has glasses
- Requires camera equipment to identify a person [9]

2.9 Facial thermography

This method was developed in the mid-1990s. Facial thermography was first used as an identification method in 1997. This method works similar to facial recognition, but an infrared camera is used to capture images. Thermographyl senses and detects thermal patterns and vessel branching. Even single twins have different termograms. The technology uses bi-sensor data to automatically and uniquely identify a person. [21] [22]

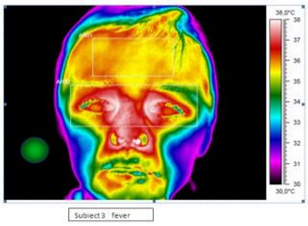

Figure 8 Facial thermography [20]

Nowadays, hand thermovision is also used to identify people, where a person can have his/her hand identified according to the map of hand or finger veins; this method is still not very widespread and is not used in aviation yet.

Advantages:

- Not intrusive technology - no physical contact is required
- Images can be captured in real-time
- The best advantage is that infrared cameras work well even in low light or full darkness

Disadvantages:

- considerably more expensive technology

2.10 DNA - Deoxyribonucleic acid

DNA has been an identifying element used mainly in police practice since the second half of the 1980s. The structure of DNA is different for all humans except for single-sex twins and does not change with increasing age. The high accuracy of DNA investigation is the reason for the wider use of this technology, despite the fact that obtaining DNA duplicates is a relatively demanding and lengthy procedure. For real-time access control or real-time identification, this technology is not applicable. [1]

Advantages:

- Very high precision, the DNA sample is the same for each cell or organ of the body
- It is impossible for the system to make a mistake
- This is a standardized verification method

Disadvantages:

- Very costly to set up
- Very disturbing method
- In terms of real-time usage, this method is still inapplicable [9]

The following table compares the aforementioned biometric systems used in aviation in terms of accuracy, cost, necessary equipment and social acceptance.

Table 1 The comparison of individual biometric methods

Biometric Technology	**Accuracy**	**Costs for Establishment**	**Required Equipment**	**Social Acceptance**
DNA	High	High	Testing Device	Low
Detection of the iris	High	High	Camera	Stredná- Nízka
Retina Scan	High	High	Camera	Low
Face Recognition	Stredná- Nízka	Medium	Camera	High
Voice Recognition	Medium	Medium	Microphone, telephone	High
Hand Geometry	Medium - Low	Low	Scanner	High
Fingerprint	High	Medium	Scanner	Medium
Face / Body Thermovision	Medium - High	Medium	Infrared Camera	High
Signature Recognition	Low	Medium	Optical Pen and Touch Panel	High

3 THE SURVEY OF CUSTOMERS´ SATISFACTION WITH THE TIGHTENING OF SECURITY CHECKS

The subject and purpose of the questionnaire survey was to assess how the public's perception of the constant tightening of security checks at airports in a handling and check in process.

A questionnaire with 10 questions to answer was used to get feedback from respondents.

The questionnaire survey was processed by 382 respondents using air transport between the ages of 16 and 67 of which 151 (39.5%), were men, and 231 (60.5%) were women.

The respondents of 83.8% perceive air transport as a safe means of transport. Only 4.2% of respondents do not consider air transport to be safe.

Currently, 51.3% of the respondents perceive the safety measures currently applied in air transport as very good and 12.1% of the respondents are inadequate.

Changing and continual tightening of security checks at airports is accepted by 54.1% of respondents positively. The tightening of security measures negatively affects 22.3% of respondents. An increase in the use of biometric technologies used at airport security checks to enhance aviation safety (iris or retina scan, facial recognition, etc.) is positively accepted by 54.1% of the participants in the questionnaire survey. The respondents of 23.1% have a negative attitude towards the introduction and use of biometric technologies, which is almost ¼ of the participants in the questionnaire survey.

For 61.8% of respondents to provide biometric data for security controls is acceptable. On the other hand, 17.4% of the respondents answered that the provision of these data is not acceptable to them. A group of 20.8% of respondents used the word "sometimes" in their response, of which it can be concluded that, under certain circumstances, the provision of these data may not irritate them, but in other circumstances people may feel offended. It can be assumed that these respondents have no knowledge that, once they have provided their data, they will be stored forever in security databases, allowing them to be accurately identified. Therefore, it is quite likely that this group of people, if sufficiently informed, could change their minds and the provision of biometric data would always be acceptable to them.

The respondents of 20.3% would welcome the mitigation of security measures when checking passengers at airports. A further 19.3% responded by a neutral answer, "maybe", and it is therefore possible to associate this group in part with those who would welcome the mitigation. However, most respondents, 60.5%, said they would not be satisfied with the mitigation of the security measures. The trend of a continual tightening of aviation security measures can negatively affect the use of air transport by 15.2% of respondents and partially 18.1% of respondents. The measures taken do not affect the selection of the means of transport - 66.7% of the respondents.

Up to 30.8% of respondents said they were worried or afraid of a possible incident. Only 42.1% of the respondents said they were not afraid of flying and the air transport was considered safe.

The professional competence and professionalism of airport staff in security controls is very well appreciated by 51.7% of respondents. 47.2% of respondents consider it to be sufficient and 1.1% of respondents are not satisfied.

Asking a question what the respondents think is the greatest risk of an airplane incident we tried to find out their biggest concern. The respondents also chose several choices to answer this question. The greatest risk of an incident is seen in a possible "technical airplane defect" which was reported by 285 of 382 respondents, representing 74.8%. On the second place, 40.2% answered "terrorist attack on aircraft from the ground or from the air". The answer "bomb on board" was reported by 35.7% of respondents and also "aircraft crew failure", was anwered by 34.8%. Concerns about "aircraft abduction" have 20.7% of respondents. Respondents had the choice of 'Others' to describe the type of threat they are concerned about. This choice was used by only 3.4% of respondents, and most of the other types of threat were: bad technical condition of the aircraft, preference for economic profitability to the detriment of aircraft reliability, adverse weather conditions such as rain, strong wind or a combination thereof, failure, staff error on the ground.

4 CONCLUSION

In recent years, aircraft accidents have constantly encouraged air transport experts to find ways to prevent them, while enhancing safety. The current trend of introducing new safety technologies is to a certain extent influenced not only by aviation personnel and air deployment workers, but also by passengers themselves. The deployment of biometric technologies in air transport can be accepted in a different way, and one can perceive it as a tool to eliminate the potential risks of an incident but also as a tool for global control and loss of intimacy. In this article, we have therefore tried to approach the use of biometric technologies in air transport from the point of view of the passengers themselves. As part of its solution, we conducted a questionnaire survey to find out how these tightening security measures and the introduction of biometrics into aviation affect ordinary travelers. The evaluation of the questionnaire survey showed that more than 80% of passengers considered air transport to be a safe means of transport. Exercise and application of biometric systems in airtransport will be negatively received by every 4 to 5 passengers. In this context, it is also important to deal with the issue of providing biometric data databases so that they are not misused.

REFERENCES

1. SZABO, S., NĚMEC, V., SOUŠEK, R.: *Management bezpečnosti letiště Brno*: Academic Publishing House CERM s.r.o, 2015, 172 p, ISBN 978-80-7204-933-2.
2. National Law Enforcement Officers Memorial Fund: *Deadliest Days in Law Enforcement History* [online]. [Cited in 2017-03-13]. Available on the Internet: <http://www.nleomf.org/facts/enforcement/deadliest.html>.
3. *Attacks on 11September 2001* [online]. [Cited in 2016-03-13]. Available on the Internet: <http://en.wikipedia.org/wiki/%C3%9Atoky_z_11._septembra_2001>.
4. SCUREK, R: *Biometric Methods of Person Identification in Safety Practice*: Study text. Ostrava: VŠB TU, Faculty of Safety Engineering, 2008. 58 p.
5. INDEX: *Capacitive swipe sensor principle* [online]. [Cited in 2017-03-13]. Available on the Internet: <http://www.idex.no/technology/swipe-sensor/#!>.
6. Advanced Card Systems: *AET62 NFC reader with fingerprint sensor* [online]. [Cited in 2016-04-05]. Available on the Internet: <http://www.acs.com.hk/en/products/130/aet62-nfc-reader-with-fingerprint-sensor/>.
7. 360 Biometrics: *What is hand geometry?* [online]. [Cited in 2017-03-17]. Available on the Internet: <http://360biometrics.com/faq/Hand-Geometry-Biometrics.php>.
8. Synerion: *Biometric time clocks. What are they? What can they do?* [Online]. [Cited in 2017-03-17]. Available on the Internet: <http://www.synerion.ca/blog/?p=1093>.
9. Advantages and disadvantages of techologies [online]. Available on the Internet: <http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of %20technologies>.
10. PALKO, P., LUKÁČOVÁ, O.: *Biometrics, the modern trend of crime detection and the tool of marketing transactions*. In: Alarm Security Magazine. Vol. 2, 2012, p. 28-31. Available online on the Internet: <http://www.infodom.com/download/AM_2_2012_CELOK_MENSIE.pdf>.
11. ANDXOR Corporation: *How is graphometric signing and verification performed* [online]. [Cited in 2017-03-17]. Available on the Internet: <http://www.andxor.com/supported-signatures.html/>.
12. MARKOFF, J., WILSON, J .: *Robot: The man behind the google phone.* In: The New York Times. [Cited in 2016-03-17]. Available on the Internet: <http://www.nytimes.com/2007/11/04/technology/04google.html?pagewanted=all&_r=1&>.
13. 360 Biometrics: *What is hand geometry?* [Online]. [Cited in 2016-03-17]. Available on the Internet: <http://360biometrics.com/faq/Hand-Geometry-Biometrics.php>.
14. Apis: Principles of Biometrics [online]. Banská Bystrica: c2011. [SA]. [Cited in 2017-03-13]. Available on the Internet: <http://www.biometria.sk/principy-biometrie.html>.
15. Biometrics Iris scaning, using eyes to identify [online]. [Cited in 2016-04-05]. Available on the Internet: <http://www.questbiometrics.com/iris-scanning.html>.
16. I-Europa: Biometrics [online]. c2003. [Cited in 2016-03-14]. Available on the Internet: <http://www.euractiv.sk/obrana-a-bezpecnost/zoznam_liniek/biometricke-udaje>.
17. Ministry of the Interior of the Slovak Republic: Passports [online]. Bratislava: MVSR. [SA]. [Cited in 2017-03-15]. Available on the Internet: <http://www.minv.sk/?cestovne-pasy>.
18. MORE, S. M.: *Biometric ePassport is cloneable*. [Cited in 2017-04-05]. Available on the Internet: <http://innovya.com/tag/technology/page/3/>.
19. ICKE, D.: *New South Wales goverment recording features for facial recognition*. [Cited in 2016-04-05]. Available on the Internet: <http://www.davidicke.com/headlines/34714-new-south-wales-government-recording-features-for-facial-recognition/>.
20. Thermology: *The value of temperature mapping*. [Cited in 2017-04-05]. Available on the Internet: <http://www.thermology.com/>.
21. *Facial termography*. [Cited in 2017-03-18]. Available on the Internet: <http://itlaw.wikia.com/wiki/Facial_thermography>.
22. KING, R.: *Explainer: Facial Thermography*. [Cited in 2017-03-18]. Available on the Internet: <http://www.biometricupdate.com/201308/explainer-facial-thermography>.