International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 17 (2016) pp 9213-9220
© Research India Publications. http://www.ripublication.com

Utilization of 3D Sensors in Biometry

Hana Talandova, Miroslav Marcanik, Michal Sustek and Milan Adamek

Abstract

The begin of this article is about biometric systems. Where writers tried to describe the basic division of Biometric systems. Following part of article will be focused on sensors issues. Where are given simple labels of scanners and 3D scanners. The next part of this article showing description of scanner usage in biometric systems (face identification, finger print, etc...). This article is focused on understanding of biometric scanning.

Keywords: 3D sensors; sensors; biometrics system.

INTRODUCTION

At this time, when advances in technology makes our lives so easier, that we rely on technology and the heavy manual work is replaced by machine. However, every technologic innovation hiding potential of hidden threats for its user. One of these threat is theft of private data and information's. Digital data are becoming increasingly widespread, users are trying to protect their data with high level encrypted password. However, abusing and theft protecting systems are rising. Disadvantage of vulnerabilities in user's data has resulted in duplication or falsification and their misuse. This rising fight with cybernetic safety led to the birth of biometric security systems. This article shows main differences between methods of biometric technologies which are used for user identity verification [1].

Section III. Is focused on construct principals of sensors. The binary system is a numbering system which is used to express a value using only characters 0 and 1. The binary system belongs to a group of positional number systems with base 2, which is a specific number as expressed by the power of 2. The numbers registered in the binary system are called binary numbers. Record of numbers in the binary system is complemented by a 'B' or 'b', which is used as a subscript on the last digit or acronym BIN [2]. Sections IV. – XI, are focused on functional advantages or disadvantages of given methods and their usage in modern times.

BIOMETRY

Biometry is modern method for user identification based on elaboration of given biometric data. These data are used for access control of buildings or databases. Biometric characteristics can be grouped as Physiologic and Behavioral, see on Figure 1 [3].

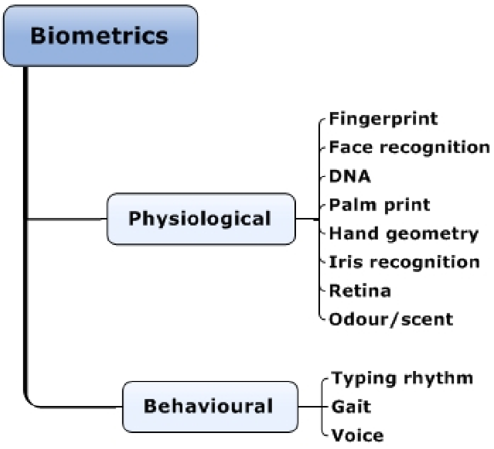


Figure 1. Distribution of biometric characteristics [3]

Biometric system could be used for identification, or verification. During verification process is user identity known and we just compare given data with data in database. It's a quick process, which has result allowing or dismissing access. During identification process we don't know user identity, we've got identification information only, this information we enter in to database request, this request is similar as verification process we comparing given data with data in database then we've get result "Match found" or "No match found". Identification process is more difficult, because this process involves comparing the entire database. Checking verification users may be supplemented with traditional methods as PIN code, electromagnetic cards, keys, etc. Dividing options of input user verification is on Figure 2 [4].

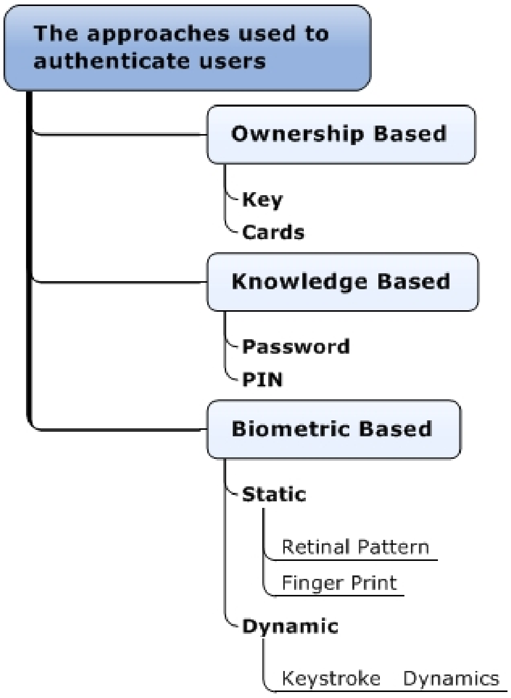


Figure 2. Distribution of access authentication options [3]

Biometric systems were first time introduced in 70's, when it comes to recognition system newly discovered biometric data given by user already saved in database. The system then evaluates, if its cheater or legitimate owner and then grant access or dismiss access to user. Biometric system works in three phases, see on Figure 3 [5].

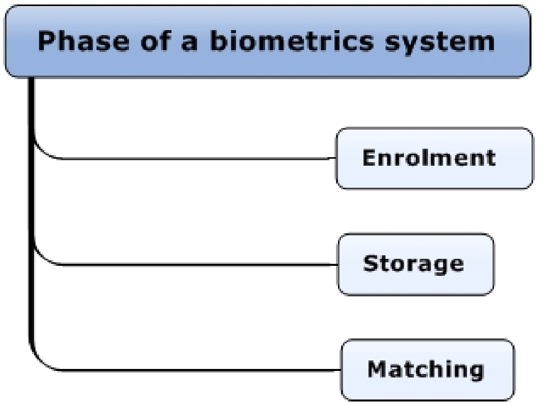


Figure 3. The main phase of a biometric system [3]

In first phase the biometric system collecting biometric data from user, data are collect and then saved to the database. Through this process must go everyone who will have access allowed in to object or database. In second phase are extracted unique or characteristic features from scanned biometric data given from first phase. In the last phase occurs validation and evaluation of access. At that moment is newly scanned biometric information of user compared witch already saved data, then evaluated and the result says if user is cheater or legitimated owner and dismiss or allow him access.

Was suggested many of biometric systems based on recognizing biometric data, their task was make safety and user interface better in all ways. Every of these systems has their own advantages and disadvantages. In case as eye scanner is, user can feel uncomfortable feeling and someone could be worry about eye. In hand geometry identification case some people with arthritis or rheumatic could have problem and in finger print case is problem with dirt or oil on fingers. Because of these issues was developed face recognizing method, which is supposed to solve it [5].

SENSORS

For first what sensors or scanners are and what they are doing? Sensors are elements, which produce input block measuring chain, then this chain is in direct contact with the measured medium. Other labels of sensors are for example sensor, detector, converter, and scanner [6].

We could order sensors by usability into categories:

- For measuring quantities;
- For physical principles;
- For the measurement environment;
- For signals according to their transformation;
- For Manufacturing Technology.

Changes of measuring quantities are scan over sensitive element mostly known as receptor, then subsequent evaluation in the sensor circuit (A/D converter), where is measured value converted mostly in to electric impulse, which could be processed or could be used directly as output quantity. Principle of sensor is shown at Figure 4.

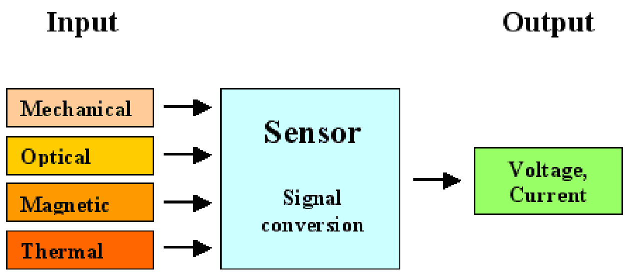


Figure 4. Principle shooting [7]

First smart sensor (1978) Beckenbridge and Husson, was defined as: Smart sensor contains functions for processing measured data, automatic correction measured data, and it could automatically detect and eliminate abnormal and wrong values. Also contains a set of algorithms, which allows to respond on changes of external conditions. We could see block diagram on Figure 2.

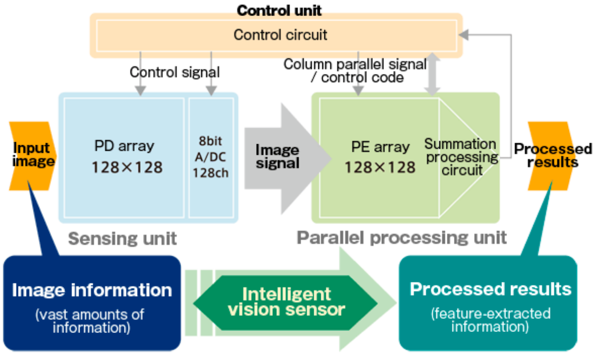


Figure 5. The principle of intelligent sensors [7]

3D sensor can be defined as a measuring unit which senses an object in 3D space or occupies angles X, Y and Z. 3D sensors operate on the principle of two or more video cameras, or for engaging the third dimension may be used most of the laser scanner. This makes possible a whole or only a certain part transform into 3D and 3D scene then analyze and select the best way to handle [6].

From the above description 3D sensor can be divided into two basic categories by using various sensors. Active and passive sensing.

- Active scanning uses laser / camera, additional information or other auxiliary devices. The concept of active sensing is very closely linked to the concept of "creating depth map".
- Passive versus active scan uses only one sensor - the camera / laser.

Since it is an improved sensor can be categorized in a similar 3D sensors. FIG. 3 we can see a general allocation [6].

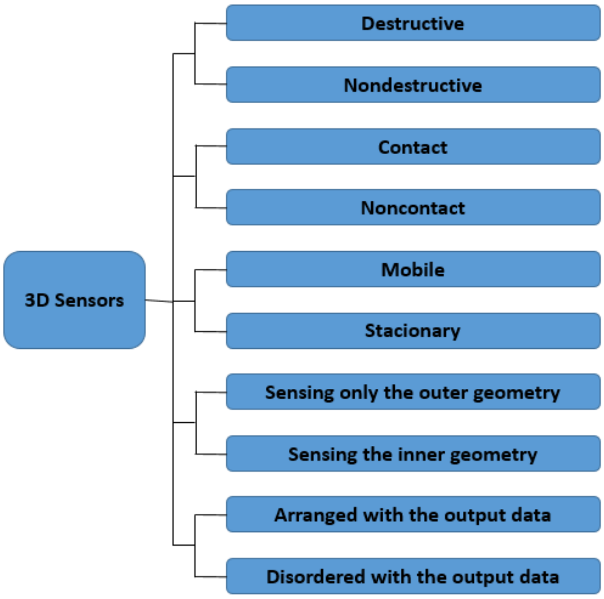

3D Sensors
Destructive
Nondestructive
Contact
Noncontact
Mobile
Stacionary
Sensing only the outer geometry
Sensing the inner geometry
Arranged with the output data
Disordered with the output data

Figure 6. Distribution of 3D sensors [6]

FINGER PRINT

This is oldest and most widely method. With the gradual development technology, we can order by:

- Ink + scanner;
- Optical;
- Optical and electrical;
- Capacitive;
- Ultrasound;
- Pressure;
- Thermal;
- Electroluminescent.

Finger printing can be divided by two basic methods:

- Static sensing finger (a) – principle is pressing a finger on the sensor.
- Dynamic sensing finger (b) – It is similar like static sensing requiring a sensor, which has the form of a small peg. After swiping your finger across the sensor creates the overall image of your finger using individual strips [1].

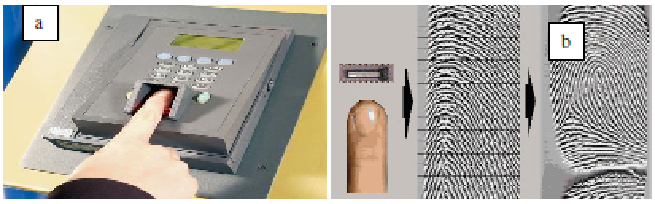


Figure 7. Static Scan (left – a), Dynamic Scan (right – b) [10]

FACE

3D face biometry provides certainty in authentication of verified user. Its very nature excludes the possibility of identity theft or other Gaming like borrowing access card to other unauthorized person or using photography [11].

- The method of measuring geometric characteristics - to identify used mostly face shape and position of visually significant places on the face (eyes, nose, mouth, chin, eyebrows), while not keeping the exact location of points, but relative distances example. Distance lips from the nose, the angle between the tip of the nose and one eye etc.
- The method of comparing patterns - comparing the image captured camera images to the database = correlation), the database is stored face like a nut brightness levels - mostly used monochrome cameras, color is used only for easier localization of human skin in an image, the lighting conditions depends on the quality the camera sometimes uses infrared region - of varying difficulty - to what extent are placed conditions on the position and orientation of the face relative to the camera, lighting conditions, the conditions placed on the background - problems - very similar people (the twins), changes of hairstyle, change grimaces glasses beard, less reliable method (rather verification) - preferably a non-contact measurements even at greater distances, unobtrusive user's individual measurement may not even know (the airport entrance halls etc.)
- The method of 3D facial measurements - identification by the 3D appearance. Scanning using a projector of structured light near-infrared and digital cameras - insensitivity to light - thanks to the use of light in the near infrared and direct measurement of absolute dimensions, this solution is sensitive to ambient light, background color or makeup face - insensitivity to angle - identification even when heads turn up to 30 ° in each direction - the uniqueness of 3D images - the amount of earned dimensions and important points is also sufficient resolution twins.

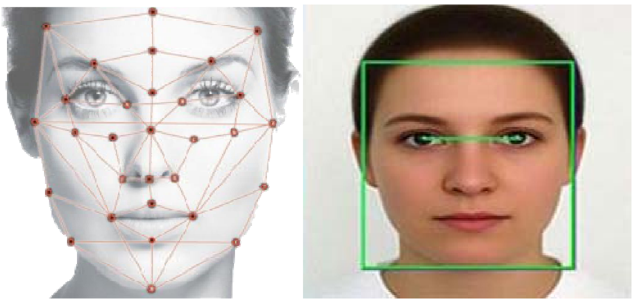


Figure 8. Face Recognition [11]

THE IRIS

It is the uniqueness of each person during the life of almost constant (stabilized during the first two years of life). The most distinguishing characteristic of man (more than 250 different detail), even unicellular twins have different iris. It is very difficult to surgically alter the iris and easy to recognize artificial - when shooting using conventional CCD camera and the method does not require any user intimate contact with the scanning device [1].

Current techniques minimum limit users:

- Camera distance of about 10-40 cm, the man is looking into the one-way mirror, once the eye is somewhat stable, the camera focuses and shoots the image.
- Personal monitor - the user holds the sensor in hand, looking into the lens, and pressing a button starts the process of identifying.

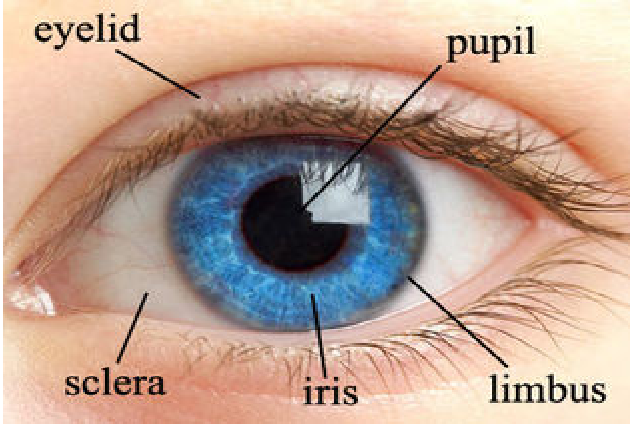


Figure 9. How Iris Scanners Record Identities [12]

THE RETINA

The retina is the light sensitive surface of the back of the eye, consisting of a large number of nerve cells, rods and cones. To verify the retina uses the image of the structure of the retina around blind spots - in comparison with the iris is much more demanding, and technical equipment and to an identified person. Because the retina is not directly visible, it is necessary to use a coherent infrared light source with low intensity (infrared radiation is rapidly absorbed by the nervous system). It is also necessary that the user looking exactly in the space and have focused on the point - providing at least the same amount of data for distinguishing a fingerprint, the retina may throughout life slightly change its structure affect some diseases (e.g. glaucoma) - little deployment system, used perhaps only in US prisons [1].

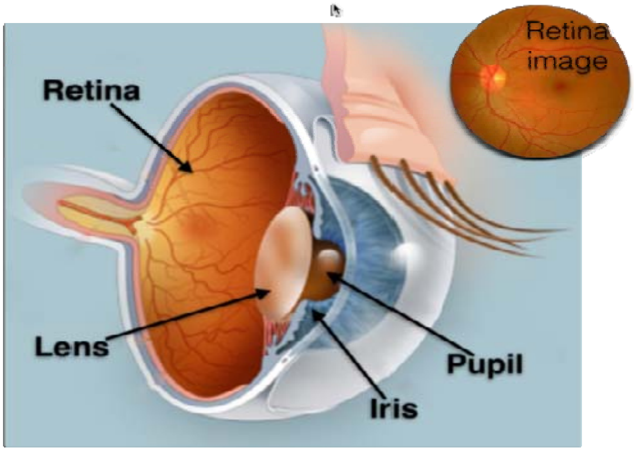


Figure 10. Principle Retina image [8]

HAND GEOMETRY

It works on the basis that each person has a different hand shape and geometry throughout life changed. They are measured symptoms such as length and width of the fingers, palm width etc., systems do not give too much data compared to e.g. A fingerprint or iris template and takes just 9B, because the systems are used rather. Not to verify identification.

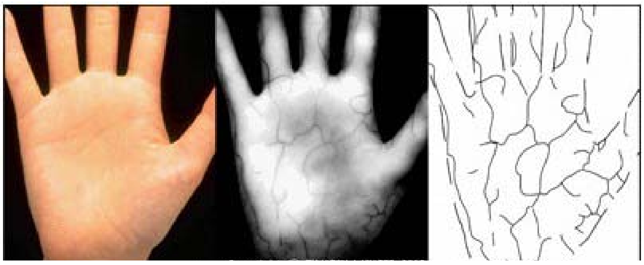


Figure 12. One example of vein scanning [1]

THE IMAGE OF THE NAIL, THE NAIL BED

Fingernail a line on the surface roughness, replicating the structure of the nail bed, which are unique for each person, each finger. With proper enlightenment we get a reflection of a "barcode". Nail bed is substantially parallel subcutaneous.

Structure located directly beneath the fingernail. Growing nail moves along the structure and copy its surface. If you look closely at your nails, you will discover different wide lines with different widths spaces. For lighting uses a beam of polarized light at the right angle, are then evaluated by phase changes beam after reflection. Treatment is intended dimensional structure of the nail bed, the numerical sequence similar to the bar code. Main big disadvantage is the low resistance email forgery.

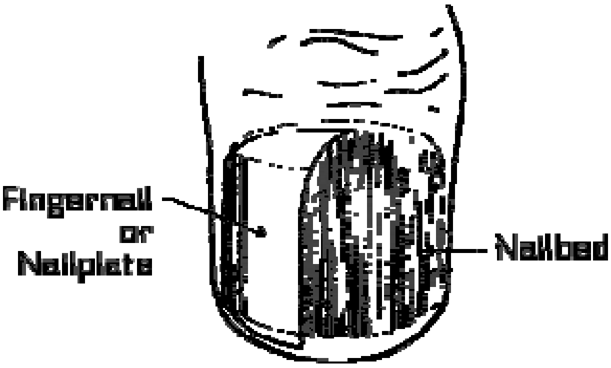


Figure 13. Principle scanning nails, nail beds [13]

HANDWRITING / SIGNATURE DYNAMICS

This is not about Digital signature, but the person must sign a special pad with a special pen. The system verifies the signature of a person based on a comparison with the stored specimen signature that describes how the signature was written. It is thus important form of signature or shape of the letters, although it can of course be used as well, but the emphasis is on the dynamics of signing, execution moves, the strength that we push when writing on a pad, typing speed, etc. All this gives an unambiguous characterization of any signature. Recognition technology is based on a comparison of changes in pressure, acceleration in different parts of the signature, pen tilt, alignment of the individual parts of the signature, the overall speed, travel time and the movement of the pen on the paper and over. Tougher against counterfeiting than the actual handwriting analysis, counterfeiters to imitate the handwriting is not enough, even watching how the question is not signed its characteristics accurately imitate. The downside is that not one person will always sign the same signature is also susceptible due to hand injuries, fatigue etc. [13].

Figure 14. Handwriting [14]

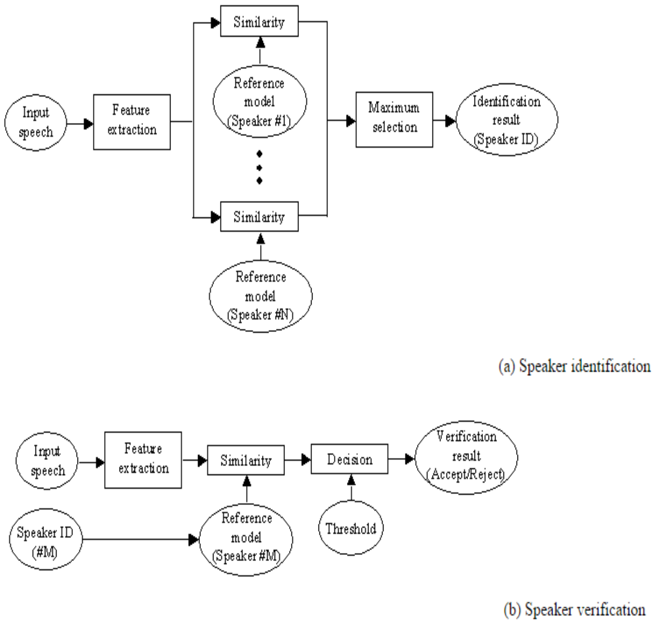
VOICE / SPEECH

Identification based on analysis of sound, vibration, pronunciation, and the speed of speech. Voice characteristics depends on the size of the vocal cords, mouth, nasal cavity, and further processes of voice Man. Used amount of flags that can be divided into two groups for statistical and dynamic.

- Statistical - independent of the text, working with long-term averages, histograms, use only voiced segments - basic tone (frequency) of speech, long term spectrum of speech, LPC coefficients (linear predictive coding), correlation and covariance matrix of individual symptoms.
- Dynamic - Suitable for speaker recognition based on the text, in terms of determining time histories of selected parameters of speech - the basic tone of the speech, the first formants, spectrum, cylindrical model of the vocal tract and others.

Some technologies are based authentication his decision on an analysis of words and whole sentences that knows

Only authentic spokesman, is thus to speech recognition and validation of knowledge passwords. It is mainly used to control access to information systems by telephone. The downside is that verification can be affected by such. Colds, fever, mental state of the speaker, noisy surroundings, etc. [14].


Similarity
Reference model (Speaker #1)
Input speech
Feature extraction
Maximum selection
Identification result (Speaker ID)
Similarity
Reference model (Speaker #N)
Input speech
Feature extraction
Similarity
Decision
Verification result (Accept/Reject)
Speaker ID (#M)
Reference model (Speaker #M)
Threshold

(a) Speaker identification

(b) Speaker verification

Figure 15. Basic structures of speaker recognition systems [15]

CONCLUSION

We can find a lot of potential in utilization of 3D sensors in all sectors from an overall perspective. A big boom was registered mainly in the improvement of cartography, digitization, security etc. It is possible to say, that biometric technology are new technologies for most of us. Here exists many solutions and applications of biometric technology which are used in safety systems. It has a number of advantages that can improve our lives, such as: increased safety and efficiency, reduce fraud and costs of the administrator password, ease of use and allows you to live a much more comfortable. Although biometric security system still has many problems, such as information privacy, physical protection of privacy and religious objections, users cannot deny the fact that this new technology will change our lives for the better.

ACKNOWLEDGMENT

With support by grant No. IGA/FAI/2016/27 and IGA/FAI/2016/25 from IGA (Internal Grant Agency) of Thomas Bata University in Zlín. This work was supported by the Ministry of Education, Youth and Sports of the Czech Republic within the National Sustainability Programme project No. LO1303 (MSMT-7778/2014).

REFERENCES

[1] JAIN, Raj. A Survey of Biometrics Security Systems. In: WUSTL Web Page [online]. [retrieved 2016-08-02]. Available from: http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/

[2] Binary System. PLC Automatization [online]. [Retrieved 2016-07-18]. Available from: http://plc-automatizace.cz/knihovna/data/soustava/dvojkova-binarni-soustava.htm

[3] Talandová, Hana, Hana Urbančoková a Milan Adámek. The Analysis of the Physiological Similarities between Family Members. In: 2014 International Conference on Mathematics and Computers in Sciences and in Industry. Varna, Bulgaria, 2014, pp. 6-9. ISBN 978-1-4799-4324-1. DOI: 10.1109.

[4] Talandová, Hana, Hana Urbanščoková and Milan Adámek. Comparing Physiological Similarities between Fingerprints of Family Members by MorphoSmart Finger VP Scanner. In: International Journal of Circuits, Systems and Signal Processing. Volume 9. USA, Oregon: North Atlantic University Union, 2015. p. 300-305 ISSN: 1998-4464. 6 p.

[5] Talandová, Hana, Lukas Kralík a Milan Adámek. The Analysis of the Physiological Similarities Human. In: Recent Advances in Electrical Engineering and Educational Technologies. Athens 2014, pp 6-9. ISBN 978-1-61804-254-5.

[6] Marcaník M. and J. Dvorak. Use of 3D sensors for the protection of critical infrastructure elements and soft targets. Zlín: Tomas Bata University in Zlín, 2015. ISBN 978-80-7454-559-7.

[7] MEMS Sensors and Actuators: Sensors General [online]. [Retrieved 2016-08-02]. Available from: http://www.tf.uni-kiel.de/matwis/amat/semitech_en/kap_7/backbone/r7_1_3.html

[8] Hamamatsu: Sophisticated sensing technology: Intelligent vision sensor [online]. Hamamatsu Photonics K.K. [Retrieved 2016-08-02]. Available from: https://www.hamamatsu.com/us/en/technology/innovation/ivs/index.html

[9] Biometric analysis of the eye in handheld devices [online]. iElectrons, 2014 [Retrieved 2016-08-02]. Available from: http://www.intelligentelectrons.com/journal/2014/1/10/biometric-analysis-of-the-eye-in-handheld-devices

[10] Indiamart: biometric fingerprint scanners [online]. IndiaMART InterMESH Ltd. [Retrieved 2016-08-02]. Available from: http://dir.indiamart.com/pune/biometric-fingerprint-scanners.html

[11] Functionspace: Face Recognition [online]. IndiaMART InterMESH Ltd. [Retrieved 2016-08-02]. Available from: http://functionspace.com/quartertopic/957/Face-Recognition

[12] Injes [online]. biometricsfingerprintreader.com [retrieved 2016-08-02]. Available from:

http://www.biometricsfingerprintreader.com/ photo/pl3158274-usb_ir_camera_eye_ detection_biometric_iris_scanner_15_20cm_ iris_capture_range.jpg

[13] Biometrics: mainguet [online]. Jean-François Mainguet, 2004 [cit. 2016-08-02]. Available from: http://biometrics.mainguet.org/types/ nail.htm

[14] Howstuffworks: How Biometrics Works [online]. TRACY V. WILSON [cit. 2016-08-02]. Available from: http://science.howstuffworks.com/biometrics 1.htm

[15] An Automatic Speaker Recognition System [online]. [Retrieved 2016-08-02]. Available from: http://minhdo.ece.illinois.e du/ teaching /speaker_recognition/speaker _recognition.html