BIOMETRIC IDENTIFICATION OF PERSONS

Milan Adámek, Petr Neumann, Dora Lapková, Martin Pospíšilík and Miroslav Matýsek
Tomas Bata University in Zlín
Faculty of Applied Informatics
Nad Stráněmi 4511, 760 05, Zlín, Czech Republic
E-mail: adamek@fai.utb.cz

KEYWORDS

Biometric systems, reliability, attack, fake fingerprint, dactyloscopy.

ABSTRACT

Algorithms - used for the identification and verification of individuals through fingerprint recognition technology have long been extensively used in Forensic Science and in the private sector. This work is concerned with the verification of the reliability of biometric systems that use fingerprints for their activities. Further, the eFinger programme is used to study similarities between men, women´s and family members´ fingerprints.

INTRODUCTION

Biometrics has been used since ancient times to recognise/distinguish people. People mutually recognised each other by voice, face or the way they walked. Some characteristics do not change during human life; while others, on the contrary continue to be shaped with increasing age [1].
Differentiating people by their fingerprints is one of the oldest Biometric recognition methods. From the earliest times, this method was used by a lot of civilisations that had some form of knowledge of papillary lines, which are included on human skin. The first provable evidence of the use of modern Biometrics however, dates back to somewhere around the mid-19th Century. This was when fingerprints began to be used in Criminology. William James Herschel was one of the first people to take advantage of Biometrics then. He used railway employees´ fingerprints to confirm their identity. Using fingerprints was the only possible way to prove the identity of individual workers, because the majority of them could neither read nor write - and therefore, one could not expect a signature from them. This fingerprint confirmed their identity when being paid their salary.
In 1865, Francis Galton came out with a "Study of the Inheritance of Physical Characteristics." The study dealt with the issue that newly-born babies take over and inherit some characteristics/properties from their parents. These characteristics can include both physical characteristics, as well as some properties - such as, behaviour or conduct. In 1869, Galton became co-founder of the science called Eugenics, which is the Science of Hereditary Diseases and Defects in the Foetus. A year later, Galton became the founder of research into twins. In 1880, he came up with a branch of science called Anthropometry, which deals with the measurement of human body dimensions. In 1892, Galton published his work entitled "Fingerprints", which led to the introduction of fingerprinting into practice in 1900. In the same year, Galton advocated the use of fingerprinting for identification and verification purposes. He demonstrated the permanence - and uniqueness, of papillary lines on the fingers. After this, fingerprinting/Dactyloscopy was introduced into police work [1].

BIOMETRICS

In Biometrics, several terms exist that are (also) used in Security Technologies. These include identity, identification, authentication, authorisation, verification, and recognition/recognisance. The term Biometrics, is a combination of two words - the word "bio" = life, and "metric" = measurement. Overall then, Biometrics can be seen as a science that deals with the measurement and examination of "live" human characteristics [1] [2].
The notion of identity is derived from the word "idem" - the same. This term is used when - for instance, comparing an object, situation, concept, and such like. One can divide "Identity" into two types; namely, "electronic identity" and "physical identity". One can have several "Electronic Identities" at the same time – e.g. an identity registered on a Web-site. Conversely, (with regard to) "Physical Identity", we each have only one, which is unique. Two people, who should have/share the same physical identity, do not exist. It composed of physiological, anatomical and behavioural traits [2][3].
Identification represents the process of discovering and identifying the validity of individuals. To begin with, the person must register such that it passes-on one´s biometric data into the system, which is stored in a database. In the course of determining the identity of a person, a comparison of the information stored in the database (template) and the currently-scanned information (sample) is carried out. This comparison process for as long as it needs to find compliance with data in the database. The output is either - finding the identity … and authorisation to enter; or to refuse entry because there was no consensus in the data.

Proceedings 31st European Conference on Modelling and
Simulation ©ECMS Zita Zoltay Paprika, Péter Horák, Kata Váradi,
Péter Tamás Zwierczyk, Ágnes Vidovics-Dancs, János Péter Rádics (Editors)
ISBN: 978-0-9932440-4-9/ ISBN: 978-0-9932440-5-6 (CD)

BIOMETRIC IDENTIFICATION METHODS

For Biometric identification needs, the human body can be divided into several basic components – or fields. These include the head, the arm/hand(s), the leg/foot/feet, and others. For personal identification purposes, one can make use of the methods set out in the table below.

Table 1 Comparison of Biometric Methods [1][4][5]

Method	Field of Use		Interfaces with Users	Characteristics		Accuracy
	P-S	B-K		A-F	B	
Scanning Faces	+	-	The face is scanned from a distance up to 2m	+	-	●●
Irises	-	+	Looking into the camera from a distance of cca. 30 cm	+	-	●●●
Retina	-	+	The eye is focused on the centre of a sensor at a distance of about 2 cm	+	-	●●●
Outer Ear	+	+	Users sets their ear close to a sensor	+	-	●●
Voice and Speech	+	+	Users pronounce words or phrases into a sensor	-	+	●
Fingerprints	+	+	Fingers are pressed on the surface of a sensor	+	-	●●●
Palm-prints	+	+	Palms are pressed on the surface of a sensor	+	-	●●●
Scalloping of Nails	-	+	Fingers are inserted into a special sensor	+	-	●●●
Veins on the Back of the Hands	-	+	Hands are inserted into a sensor	+	-	●●
Veins in the Palm of a Hand	-	+	A palm is placed into a sensor	+	-	●●
Veins in the Fingers	-	+	Fingers are inserted into a sensor	+	-	●●
Signature Dynamics	+	+	The signature is made with a special pen on a special surface	-	+	●
Computer Key-stroke Dynamics	-	+	Users write a sample text on a special keyboard	-	+	●●

P – **For Policing - Forensic Identification**
B – K **For Safety - Commercial Identification**
A – F **For Anatomical - Judicial Characteristics**
B – **For Behavioral Characteristics**
P – S **For Police – Court Identification**

The human body undergoes many changes, whereby some properties/characteristics are more – or less, dependent on stability in time. The two most consistent properties over time - include the (human) iris, and DNA – in which almost no change occurs. Conversely, the characteristics of the human voice change a lot throughout life - especially during puberty. The time constancies of these biometric characteristics are depicted in Figure 1; the degree of temporal stability is expressed in percentages [4], [7].

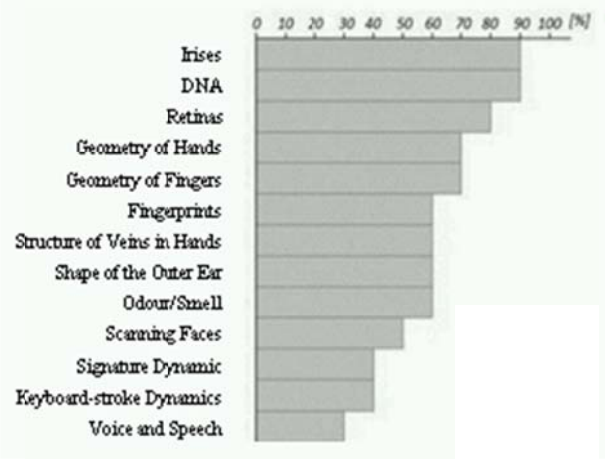

Figure 1: The Degree of Human Biometric Temporal Stability - expressed in percentages

BIOMETRIC SYSTEMS

The basic component of a Biometric Identification System (BIS), is a sensing module that ensures the scanning of biometric characteristics. The core part is the decision-making module, which compares the biometric features defined in the database. The output of

the biometric identification system is the communication interface, or "lock" - allowing access to the space provided.

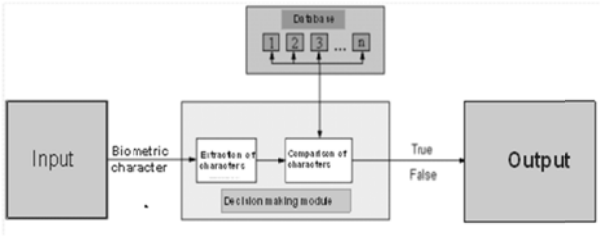

Figure 2: Structure of a Biometric Identification System, [5]

BIOMETRIC SYSTEMS´ RELIABILITY

One of the important characteristics of biometric systems includes the ability to clearly and faultlessly identify the identity of the rightful user - who is officially stored in a system database - and also, to differentiate/identify any unknown persons. Two parameters are used to express the degree of reliability of the system; these are:

- FRR – **False Rejection Rate** – (probability of erroneous rejection) – sometimes, the term also used for this is: Type I Error Rate
- FAR – **False Acceptance Rate** (probability of erroneous rejection) – sometimes, the term also used for this is: Type II Error Rate [4][6].

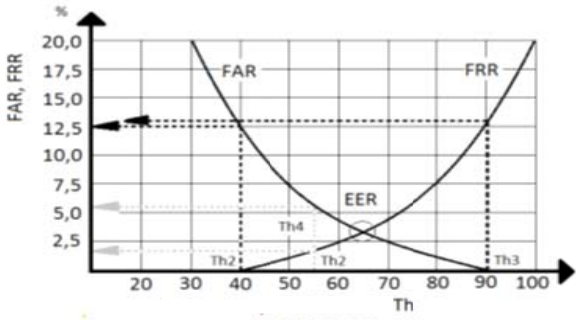

Figure 3: Dependence of FAR and FRR on Sensitivity Threshold, (Th) [4]

The False Acceptance Rate (FAR), and False Rejection Rate (FRR), and express the probability of the occurrence of a given error in percentages. From these errors, it follows that the higher the FRR - the lower the FAR; and vice versa. FRR and FAR are both dependent (Figure 3.), at the "Threshold Value". The setting of the "Threshold Value" depends on the use of the system in practice; that is to say, if the bigger problem is if someone erroneously accepts or rejects it. When FAR and FRR the values are equal, this equality is referred to as the EER - Equal Error Rate. The EER allows one to determine the "approximate value of a security system."

FINGERPRINT SENSOR PRINCIPLES

A. Optical Fingerprint Sensors

Optical fingerprint sensors are based on the reflection, or transmission of light. These sensors exploit the use of different reflections of light from papillary lines - and the space between these lines. The reflected light is then evaluated through a CCD or CMOS sensor.

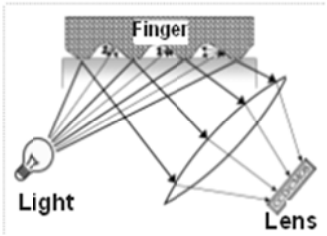

Figure 4: An Optical Sensor based on the principle of Reflections [3]

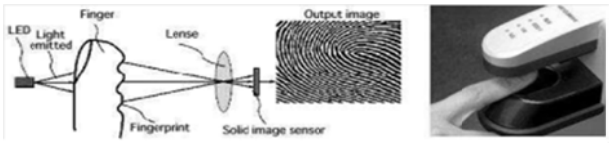

Figure 5: An Optical Sensor based on a Scanning Transmission, [3]

The optical sensor - using light transmission, is based on the backlighting of a finger from the upper side (from the nail), and on recording the sensor´s image on the opposite side.

B. Capacitive Fingerprint Sensors

The principle of this sensor is based on measuring the differences in capacity between the sensor-plate and the finger. The sensing area is equipped with a large number of sensor micro-electrodes in order to evaluate the capacity difference between the peaks and recesses in the papillary ridges in a finger.

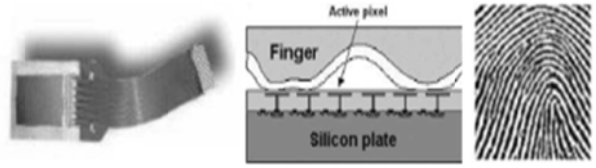

Figure 6: The Principle of a Capacitor Sensor [3]

C. Thermal Fingerprint Readers

Thermal fingerprint scanners use a small "pyro-detector" as a heat-sensitive element. The principle of this technology is based on measuring the temperature difference between peaks and valleys in finger papillary lines.

Figure 7: The Principle of a Thermal Sensor [4]

D. Ultrasonic Fingerprint Readers

This sensor transmits an ultrasonic signal from the transmitter to the fingerprint. The signal captures the reflected and deformed waves by rotating the transmitter or receiver. These are then evaluated farther and captured.

Figure 8: An Ultrasonic Reader + sample [5], [8]

FALSE FINGERPRINT-MAKING METHODS

Two approaches can be used for false fingerprint production:

1. Fake fingerprints can be created directly using appropriate materials. Several materials can be used to create a fake fingerprint - with regard to the preservation of papillary lines including their characteristics.

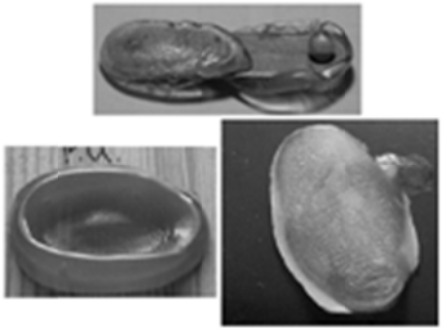

Figure 9: Plastic Finger-prints (Gelatine, Silicone, Plastic Moulds).

Granulated plastic can be used for the production of this material, which is malleable after being warmed up. Plastic materials have similar properties. Original fingerprints are pressed into plastic materials - thereby creating fake fingerprint templates. The fake fingerprint template is filled with materials like gelatine, silicone or plastic.

2. False Impressions Created by Secured Latent Traces

In order to produce a fingerprint, a "latent print" needs to be highlighted - and pictures taken – i.e. a scan; the resulting image is inverted and trimmed and then rendered in black and white shades. Enhanced image transfer of the material is designed to create a form that can be used for to "screen print" a plastic material - or create rubber stamps, etc.

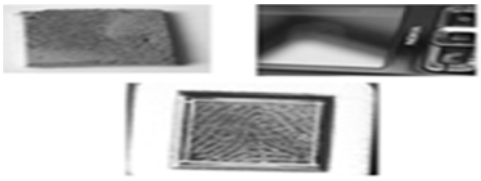

Figure 10: A Fake Fingerprint; Latent Fingerprint on a Mobile Phone.

Both procedures can create relatively high-quality fingerprints - but do not have a long shelf-life - they cannot be used with Vibrancy Control scanners. For example, gelatine or silicone cannot be applied to all touch sensors, because some methods do not meet the properties of materials that remain close to human skin properties, etc.

TESTING FINGERPRINT SENSOR RELIABILITY WITH THE USE OF FAKE FINGERPRINTS

The false fingerprints were measured against the immunity of fingerprint sensors. A Capacitive Fingerprint Sensor was used for testing the false fingerprints. The "fake fingerprints" were made from a plastic material rubber stamp.

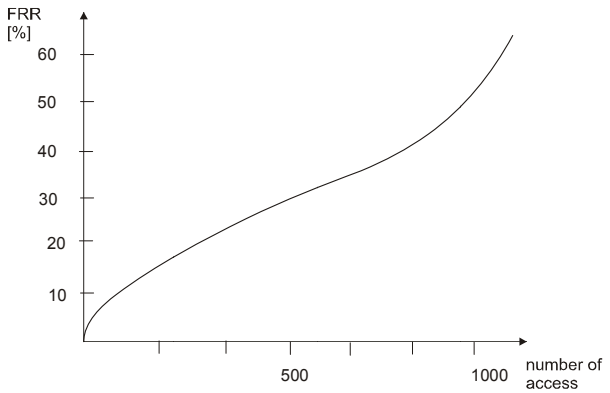

Figure 11: FRR of Capacitive Fingerprint Sensor: A fake fingerprint made from a rubber stamp

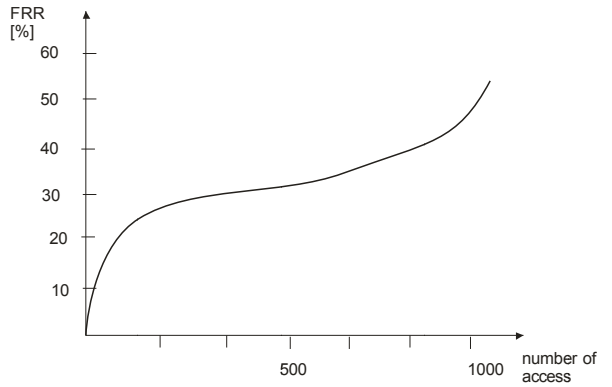

Figure 12: FRR of a Capacitive Fingerprint Sensor: The fake fingerprint is made from plastic

COMPARING THE MATCHING OF FINGERPRINTS

The eFinger programme was used for the comparison of fingerprints. The papillary ridge lines and points were extracted from a set of fingerprints stored in the database; the results are shown in Figure 13.

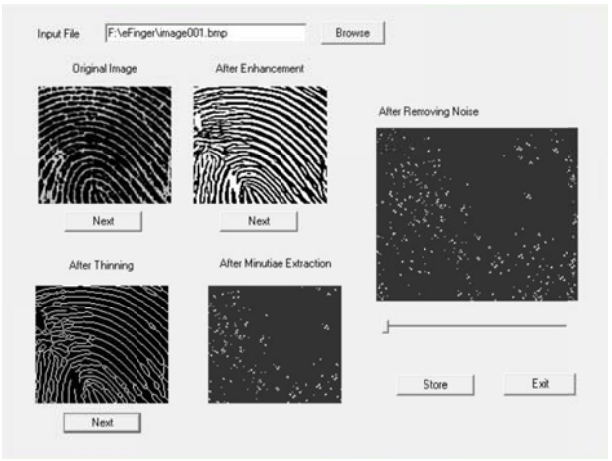

Figure 13: Extracted Fingerprint Papillary Ridge Lines and Points

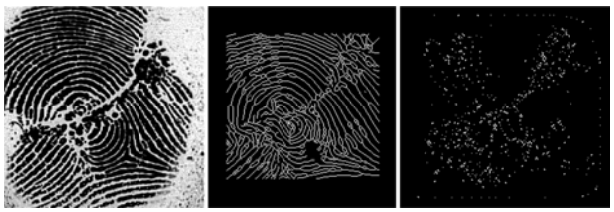

Figure 14: Demonstrations of the course of fingerprint extraction

Euclidean Metrics were used for the comparison of the match in identity of fingerprints – in which, the Euclidean Distance between Two Points, A and B is given by:

$$\rho(A,B)=\sqrt{(a_1-b_1)^2-(a_2-b_2)^2} \qquad (1)$$

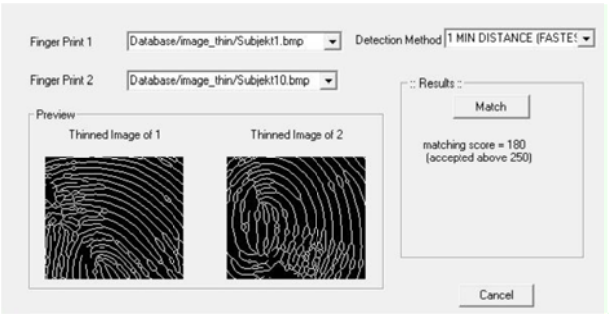

Figure 15: Mutual Comparisons of Two Fingerprints

For the MIN DISTANCE methods used in the eFINGER programme, consensus is expressed numerically in intervals ranging from 0 to 1000. The maximum match is expressed by 1000; that is to say, there is 100% concordance of the two fingerprints. In this programme, values below 250 are considered unsatisfactory. Upon reaching the minimum number of matches - expressed by a number greater than 250, the comparison of the fingerprints reaches the minimum number of matching markers.

7 women´s, (Subjects: S1, S3, S4, S5, S6, S8 and S15); and 9 males´, (Subjects: S2, S7, S9, S10, S11, S12, S13, S14 and S16), fingerprints were matched and compared.

Table 2. Comparisons and Matches in Fingerprints in Women

	S1	S3	S4	S5	S6	S8	S15
S1	1000	217	217	202	218	188	140
S3	241	1000	225	256	209	246	224
S4	250	249	1000	194	234	193	165
S5	247	247	250	1000	225	235	166
S6	226	233	238	236	1000	212	154
S8	229	220	213	192	235	1000	220
S15	234	208	231	207	200	193	1000

Table 3. Comparisons and Matches in Fingerprints in Men

	S2	S7	S9	S10	S11	S12	S13	S14	S16
S2	1000	205	218	193	182	181	196	210	171
S7	229	1000	214	181	187	195	161	193	189
S9	247	224	1000	192	175	172	203	233	163
S10	214	291	229	1000	190	190	186	211	174
S11	144	137	138	137	1000	233	244	128	127
S12	178	163	164	170	189	1000	274	172	182
S13	222	191	240	222	141	183	1000	251	157
S14	164	131	201	146	161	185	182	1000	153
S16	167	161	173	173	190	201	168	146	1000

From the tables above, it shows that, when comparing fingerprints, women show a higher degree of matching fingerprints; unlike the men´s fingerprints. Despite this, the rate of matches between individual subjects does not exceed the value of 300; that is to say, the fingerprint comparison of subjects matched the minimum number of markers T.

Table 4. Comparisons and Matches in Fingerprints between Family Members

	S2	S10	S4	S7	S15	S5	S6	S12	S13
S2	1000	193							
S10	214	1000							
S4			1000	206	165				
S7			200	1000	146				
S15			231	213	1000				
S5						1000	225	171	182
S6						236	1000	163	195
S12						159	166	1000	274
S13						201	178	183	1000

Furthermore, an assessment was made for matches and compliance between the fingerprints of family members. Subjects S2 and S10 are siblings - brothers. Subjects S4, S7 and S15 represent another group of family members - a brother, sister and cousin. The last, yellow coloured group in Table 4 is made up of Subjects S5, S6, S12 and S13. This quartet is composed of a brother, sister, mother - and their cousin). From the table above, when comparing the cardinal fingerprint elements of family members, there is seemingly no strong match between family members. Even in this case, the match compliance rate is less than 250, so – a sufficient number of fingerprint comparison markers cannot be matched, or made.

CONCLUSION

Biometric systems are closely-linked to reliability, which is given by the values: FAR and FRR. The aim of this paper was to suggest ways that can significantly impair the reliability of Biometric Systems. One such example (presented), is the production of false fingerprints – e.g., by using plastic and rubber models. Some types of fingerprint sensors are unable to recognise fingerprint copies, thus significantly impairing the reliability of Biometric Systems. Furthermore, the study also resolves the question of consensus (matching) – or respectively, the similarity of fingerprints for women and men, and between family members. The eFINGER programme was used to tackle this issue. It is based on Euclidean Distance Metrics when comparing individual points. Even a very small set of fingerprint comparisons shows that fingerprint-matches between family members are very low. Fingerprints matches only on a minimum number of minutia. Thus, they can be distinguished from one other.

ACKNOWLEDGMENTS

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) and also by the European Regional Development Fund under the project CEBIA-Tech No. CZ.1.05/2.1.00/03.0089

REFERENCES

[1] RAK, R. *Biometrics and identity of people: the forensic and commercial applications*, BEN, Prague, 2008. ISBN 978-80-247-2365-5.

[2] COUFAL, T. *What is FingerChip* [online]. 2007. <http://hw.cz/teorie-praxe/art2020-co-je-fingerchip.html>.

[3] BITTO, O. *Encryption and biometrics: or arcane bits and touches*.: Computer Media, 2005. ISBN 80-86686-48-5.

[4] LI, Haizhou, Liyuan LI a Kar-Ann TOH. *Advanced topics in biometrics*. New Jersey: World Scientific, c2012, xv, 500 s. ISBN 978-981-4287-84-5.

[5] JORGENSEN, Z a T. YU. *On Mouse Dynamics as a Behavioral Biometric for Authentication*. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. 2011; 476-482

[6] AHMED, Awad E. Ahmed a Issa TRAORÉ. *A New Biometrics Technology based on Mouse Dynamics*. IEEE Transactions on Dependable and Secure Computing. 2007; 4: 165-179.

[7] NAZAR, Akif, Issa TRAORÉ a AHMED Awad E. Ahmed Inverse *Biometrics for Mouse Dynamics*. International Journal of Pattern Recognition and Artificial Intelligence. 2008; 22: 461-495.

[8] Fujitsu Palmsecure. Fujitsu [online]. 2014. <http://www.fujitsu.com/cz/solutions/high-tech/palmsecure/>.

AUTHOR BIOGRAPHIES

MILAN ADÁMEK graduated in 1990 from the Olomouc Palacky University, Czech Republic. He received his Ph.D. degree in Technical Cybernetics at Tomas Bata University in Zlin in 2002. From 1997 to 2008 he worked as senior lecturer at the Faculty of Technology, Brno University of Technology. From 2008 he has been working as an associate professor at the Department of Electronic and Measurement, Faculty of Applied Informatics of the Tomas Bata University in Zlín, Czech Republic. Current work covers following areas: power lines, camera system, sensors. His e-mail address is: adamek@fai.utb.cz.

Petr NEUMANN has been graduated from the Brno Technical University in Electronic Technology in 1974. He has acquired the industrial experience in the field of medical electronics and quality management as R&D engineer. He received his Ph.D. degree in Technical Cybernetics at Tomas Bata University in Zlin in 2001. He has been lecturing and working in the university research area since 1994. He was engaged in the SMT technology training, equipment installation and servicing more than 10 years between 1997 and 2009. He is currently working as a senior lecturer at Tomas Bata University in Zlin. His research work is aimed at the electronic component authenticity analysis and failure diagnosis. His e-mail address is: neumann@fai.utb.cz

DORA LAPKOVÁ has been graduated from the Tomas Bata University in Zlin in 2012. Her scientific research is oriented into professional defence and self-defence, physical security and physical security technical equipment. Her e-mail address is: dlapkova@fai.utb.cz

MARTIN POSPÍŠILÍK graduated in 2008 from Czech Technical University in Prague, Czech Republic, in Microelectronics. Having received his Ph.D. degree in Engineering Informatics at Tomas Bata University in 2013, he became an assistant and researcher at the Department of Computer and Communication Systems of Faculty of Applied Informatics of the Tomas Bata University in Zlín, Czech Republic. His current research covers the following topics: electromagnetic compatibility, shielding effectiveness of materials for avionics, design of construction of electrical circuits and testing of electrical devices considering the security of communication. The security issues are investigated in cooperation with Escola Superior de Tecnologia e Gestão, Beja, Portugal. His e-mail address is: pospisilik@fai.utb.cz.