Improving the Security of Internet Banking Applications by Using Multimodal Biometrics

[1]Cătălin LUPU, [2]Vasile-Gheorghiță GĂITAN, [3]Valeriu LUPU
[2,3] "Stefan cel Mare" University of Suceava, Romania
[1]*catalinlupu@seap.usv.ro*, [2]*gaitan@eed.usv.ro*, [3]*valeriul@seap.usv.ro*

***Abstract*–Online banking applications are used by more and more people all over the world. Most of the banks are providing these services to their customers. The authentication methods varies from the basic user and password to username and a one-time password (OTP) generated by a virtual or a physical digipass. The common thing among authentication methods is that the login wepage is provided through a secure channel. Some banks have introduced (especially for testing purposes) the authentication using common biometric characteristics, like fingerprint, voice or keystroke recognition. This paper will present some of the most common online banking authentication methods, together with basic biometric characteristics that could be used in these applications. The security in internet banking applications can be improved by using biometrics for the authentication process. Also, the authors have developed an application for authentication of users using fingerprint as the main characteristic, which will be presented at the end of this paper.**

Keywords: **Internet banking, biometrics, digipass, fingerprints, security**

I. INTRODUCTION

The internet-banking concept is now part of our lives. It is easier to make transactions and to check the account status from your home than to go to a bank or to call a bank-officer. Almost all important banks are providing these kind of services to their clients. This is why the banks have to take into the account the security improvement of the authentication and signature tasks. Authentication can vary from a simple username and password (that is the weakest method) to private certificates and dynamically generated passwords (also called OTP – one time password). However, most of these methods are based on what user remembers (a password) or has (a digipass to generate an OTP). It could be easier to use something that user always possesses and that cannot be forgotten or lost. That's why biometrics are suitable for authentication in such a sensitive domain as internet banking.

Biometrics have proved that can be used in different applications, such as access control (in a building or in a car, for example), computer logon, for government applications, such as biometric passports, or for forensic purpose, such as corpse identification or criminal investigations. They are also used for airport or border security check. This proves that biometrics can be taken into account for securing the authentication in internet-banking applications.

The idea of using biometrics for online banking authentication is not a new idea, but there were not deep researches in this field. One of the most interesting paper on this field is represented by [5], where is presented a comparative study in using biometrics for banking. The conclusion of this paper is that the end-user applications are not quite developed, the main interest being the use of biometrics for access control, branch banking or at ATMs. Using biometrics for internet banking is on the fourth place, with a proportion of 10% from the cases studied (121 banks from all over the world that use biometrics for various purposes). Other personal studies are presented in [1] and [3].

In the following paragraphs, we will present some important considerations on online banking applications, together with the some of the most used biometrics that are suitable for online use. On the paragraph regarding fingerprints we will present some of our researches in development of an optimal filter through convolution methods, necessary for restoring, correcting and improving fingerprints acquired from a sensor. In the end of this paper, we will present an application developed by us, which can be used in internet banking authentication.

II. ONLINE BANKING APPLICATIONS

Online banking (with its synonyms internet-banking, e-banking, virtual banking or private banking) stands for an application provided by banks to their customers, in order to manage their own accounts and to make payments, see or download account statements or to see or make operations related to associated credit cards.

In Figure 1 it is presented a classical internet banking authentication webpage, where user has to introduce the username and a static or a dynamically-generated password (OTP). Devices called digipasses or tokens dynamically generate the OTPs (one-time passwords, valid for a short period of time, e.g. 30 sec.), based on an internal algorithm. The digipasses are associated with the user and could be opened by using a PIN (like photos 1, 2 and 4 from figure 2) or not (only by pushing a button, like the case in photo no. 3).

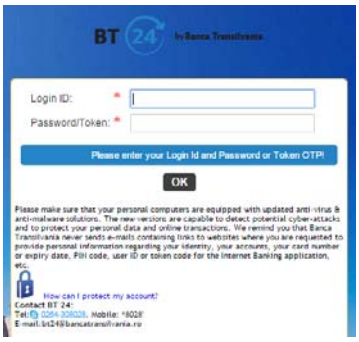


Fig. 1. Classical internet-banking authentication webpage

Fig. 2. Digipasses used for OTP generation (BCR, ING, OTP and Banca Transilvania)

The PIN is set at the bank office, when the user receives this device. The main problem is that this PIN can be forgotten, lost or stolen. This doesn't happens with the biometric characteristics, that are always attached to the user. Another possibility is that, in order not to forget the PIN or username, the user will write these credentials on the device itself, leading to the possibility that a malicious people to use them in order to access the user's account. This is one of the most important issues regarding tokens, because if the device is lost or stolen, and someone's using credentials to access the account, then the real user can't even know about this thing (not having anymore the device) and thus won't announce the bank in order to block the access.

Most of these devices are produced by the company VASCO and are personalized by each bank. In Figure 2 are presented 4 digipasses used by the major banks.

After the successful login, the main page is opened. From this page, the authenticated user can: see a quick overview on all account, search for transactions, see the statements, make some operations, like internal transfer, payments, bill payments, foreign currency exchange or transfer, constitutes or clears a deposit, sign orders and have access to information about loans. In the figure 3 it is presented the dashboard of the internet banking application. Signing an order can be done by using the static password or an OTP.

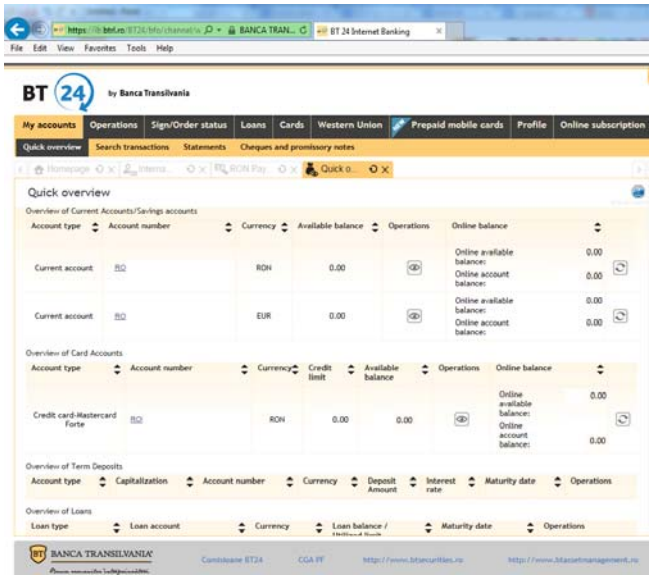


Fig. 3. Internet banking application dashboard

Next it will be presented some important biometrics that are suitable for our purpose, namely for internet-banking authentication.

III. Choosing Biometrics suitable for Internet-Banking Authentication

Biometrics have been used at the beginning for forensic purposes only. However, over the years, they started to be used for other applications, like access control or government applications.

Biometric characteristics can be behavioral (gait, signature, keystroke) or physical (fingerprint, face, hand geometry, iris, retina, vascular patterns, DNA). Some of them are suitable to be used for online authentication, while some aren't admissible for this task. In addition, some of them can use the existing resources (like voice, face or keystroke), while others need specialized devices to capture the characteristic (for fingerprint, iris or retina). The last ones involve greater costs for the user or the company that intend to use them. However, it is obvious that greater costs will lead almost all the time to better results in increasing and reach the desired security. Extended studies on biometrics are presented in books [6], [7] and [10]. Next it will be presented two important biometric characteristics: fingerprints and iris.

A. Fingerprints – one of the oldest authentication method

Fingerprints and fingerprinting have been used at the beginning for forensic purposes, since mid-19th century. They started to be used for authentication purposes with the technological progress in creating smaller devices that can be easily used. One of the firsts paper in fingerprints was [8], published in 1892 by Sir Francis Galton.

Fig. 4. Fingerprint sensors

Fig. 5. Author's fingerprints acquired using Microsoft Fingerprint Scanner

Most of the important researches about fingerprints are published in books [8]-[10], and in our personal papers [2] and [4].

In the next figure are presented two fingerprint sensors, the one in the left using the "sweep" technology (integrated on an optical mouse), while the one in the right side is a Microsoft Fingerprint Scanner, that is an optical device. The last one was used to acquire the fingerprints from figure 5, and to develop the application presented in the 4th paragraph.

Next, it will be presented the development of an optimal filter through convolution methods, necessary for restoring, correcting and improving fingerprints and eye acquired from a sensor, able to provide the ideal image in the output. This paragraph is the applied study presented in our paper [3]. After the image was binarized and equalized, Canny filter is applied in order to: eliminate the noise (filtering the image with a Gaussian filter), non-maximum suppression, gradient adaptive binarization and extension of edge points edges by hysteresis. The resulting image after applying Canny filter is not ideal. It is possible that the result will be an image with very fragmented edges and many pores in ridge.

1) Case study: the construction of an optimal filter by applying some convolution filters over the initial image

In the Figure 6 is presented a set of images obtained after the application of some convolution functions with different nucleus ([14]-[17]).

The pictures represent the following:

(a)– the application of a median convolution filter with the dimensions n-4,22 and 34;

(b) application of a gaussian convolution filter with the dimension 34 and different standard deviations σ (0.3, 0.6, 0.9, 1.00, 1.20, 1.50, 1.80, 2.00, 2.10, 2.40, 2.70, 3.000 (for the digital fingerprint);

(c) application of a gaussian convolution filter and different standard deviations σ (3 , 4 , 5 , 6 , 7, 8 , 9);

(d) application of a lapacian filter with the dimension n=3

(e) application of a circular filter with dimension 34 and different radius, r= 3, 11, 34;

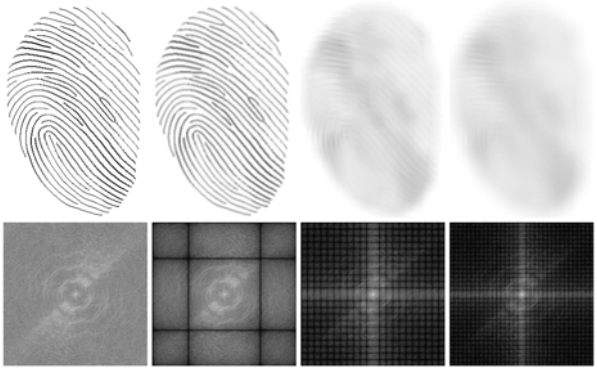
(f) application of a lapacian filter with the dimension n=3 and different values for alpha = 0.1, 0.5 and 0.9;

(g) application of a lapacian filter with the dimension n=3 over the image of the digital foorprint affected by the noise "salt and pepper", with different values for alpha σ = 0.10, 0.50, 0.90

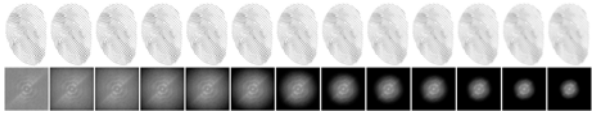
Images of the digital fingerprints after the application of the median filters with the dimensions 34 and with the values for n = {4, 22, 34}, Fourier filters, images of the median filters and of the transfer functions are presented in figure 7 (([14]-[17])):.

2) Presentation of the algorithm used to obtain the optimal filter

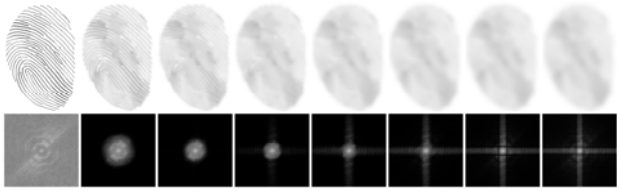
The general idea is the following: a bank of convolution filters with different nucleus is applied to the original image (with different dimensions of the convolution filter). For each feature is calculated the correlation coefficient. It is selected that feature for which the correlation coefficient is maximum. If there are more local maximum levels for different values of the features, it is selected one of these. Different banks of convolution filters are applied turn by turn (Kirsch, Laplace, Roberts, Prewitt, Sobel, Frei-Chen, average, circular, lapacian, gaussian, LoG, DoG,inverted filters, Wiener, the "equalization of the power spectrum" filter (intermediary filter between the Weiner filter and the inverted filter), the geometrical average filter, etc. For each applied filter a maximum correlation coefficient is determined. For all the convolution filters is chosen the maximum correlation coefficient among all of them. In this way the optimal convolution filter is selected that provides in the output the closest image to the ideal one.



a)

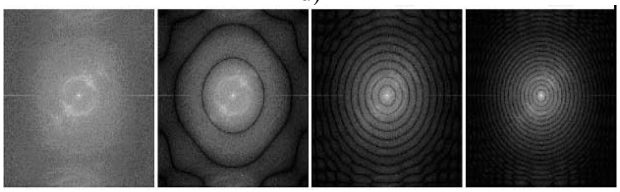


b)

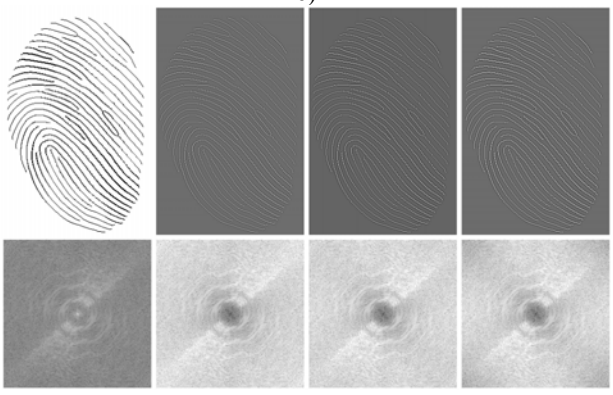


c)

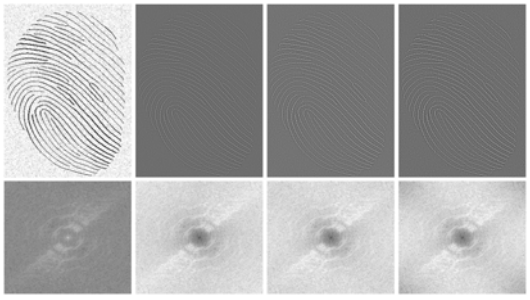
d)



e)

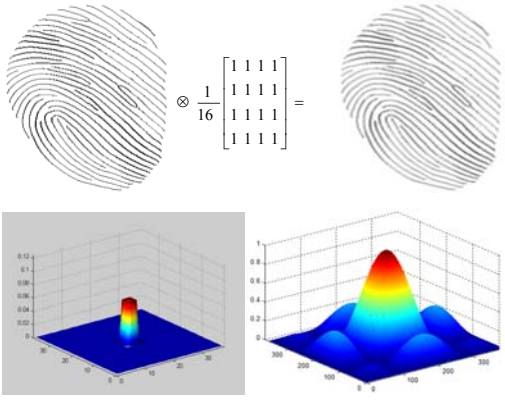


f)

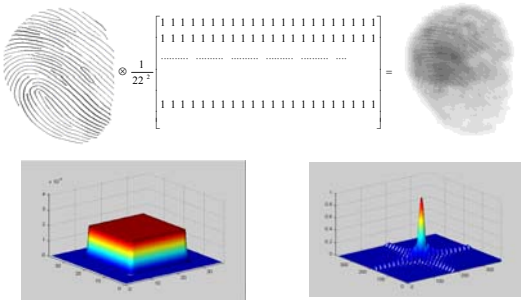


g)

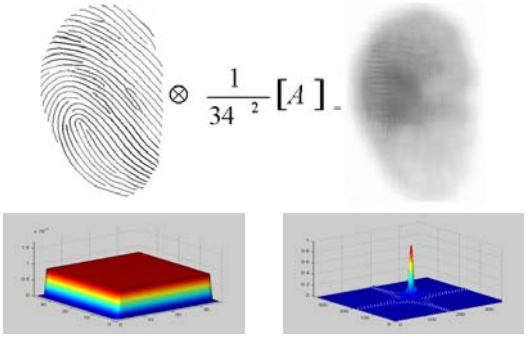
Fig, 6. The images of the fingerprints after the application of the convolution filters over the initial image.



a)



b)



c)

Fig. 7. The figures of the image 101_1.tif after the convolution of the initial image with the average filter of different dimensions (a) 4 , b) 22 and c) 34; afferent Fourier spectrus ((a) 4 , b) 22 and c) 34); images of the average filters with different dimensions of the filter (a) 4 , b) 22 and c) 34.

3) Experimental results

In the Table I are shown the experimental results of correlation coefficient between two images.

TABLE I EXPERIMENTAL RESULTS OF CORRELATION COEFFICIENT BETWEEN TWO IMAGES

Average Filter		**Circular filter**		**Gaussian Filter**		**LoG (Laplacian of Gaussian) Filters**	
Size filter	**Correlation coefficient**	**Ra-di-us**	**Correlation coefficient**	**σ**	**Correlation coefficient**	**Σ**	**Correlation coefficient**
1	1	1	1	0.3	1	0.3	1
3	**0.8243**	3	**0.9668**	0.6	**0.9784**	0.6	**0.9784**
5	0.7379	5	0.9220	0.9	0.9484	0.9	0.9484
7	0.6263	7	0.8869	1	0.9327	1	0.9327
9	0.5657	9	0.8412	1.2	0.9276	1.2	0.9276
11	0.5622	11	0.7537	1.5	0.9087	1.5	0.9087
13	0.5767	13	0.6210	1.8	0.8875	1.8	0.8875
15	0.5824	15	0.4834	2	0.8722	2	0.8722
17	0.5787	17	0.3826	2.1	0.8606	2.1	0.8606
19	0.5724	19	0.3320	2.4.	0.8264	2.4.	0.8264
		21	0.3257	2.7	0.7853	2.7	0.7853
				3	0.7394	3	0.7394
	Max=0.8243		**Max=0.9668**		**Max=0.9784**		**Max=0.9784**
Max=0.9784 (Gaussian or LoG Filter)							

4) Conclusions on the proposed method

All the methods presented above refer to the restoration of the degraded images with invariable distorting functions during the translation, using convolution methods. The optimal filter was obtained by applying the convolution filters with different features which, going from the initial image and applying to it different convolution filters, it can provide in the output an image the closest possible to the ideal one.

B. Iris recognition

The iris started to be used as a biometric characteristic after the Flom's patent, issued in 1987 ([11]). The two researchers, L. Flom and A. Safir studied the iris pattern and concluded that it is suitable for personal identification. But a more elaborate study is represented by the Daugman's patent, issued in 1994 ([12]). This patent contains very important mathematical models for searching the iris frontiers (inside and outside) and the generation of iris code using the Cartesian coordinates transformed to polar coordinates. This thing will lead to a image that is inflexible to rotation or translation. Most of the devices used to acquire iris image are still using Daugman's software to enroll or identify a person. Another important book in this field is represented by [18], published in 2013, after the Daugman's patent expired.

In figure 8 is presented a camera for iris acquirement. In the top of the camera it is an objective for iris capture, in the middle it is an objective for webcam (this camera being suitable both for iris, face or gait recognition) and in the lower part can be seen 3 infrared LEDs that will provide a infrared beam used for capture of the iris' image. The use of infrared light is explained in detail in paper [13]. This device is a little bit expensive that the fingerprint sensor, but iris provides a better authentication than fingerprints.

Fig. 8. Panasonic BM-ET100US iris camera and webcam

C. Multimodal systems

According to [6], a multibiometric system can have multiple sources of information: multi-sensor, multi-algorithm, multi-instance, multi-sample and multimodal (many biometrics combined, like iris, fingerprint, face, etc.).

Multiple biometric systems can be combined in order to increase the security of specific applications. In our case, using fingerprints and iris recognition will lead to an extremely enhanced authentication method, but the cost of the devices will rise consistently. Also, we can use only one of these methods, especially for impaired persons that do not possess one of these characteristic.

IV. APPLICATION FOR ONLINE BANKING ENROLLEMENT

During our researches in biometrics and their implementation in internet banking authentication process, we developed an application that can acquire the fingerprint from a specific sensor (Microsoft Fingerprint Sensor), process the image and extract features. It was developed in Java and can be accessed by using any web browser, on a desktop computer or on a notebook, as well as any mobile device (smartphone, PDA, tablet) that supports Java. In the following steps the application will be developed to acquire the fingerprint from any device, even from a mobile device, using in this way the existing resources.

After the successful acquirement and process of the fingerprint, it is stored in a database (enrollment) or is compared against other fingerprints in a MySQL database in order to verify (that is a 1:1 comparison, user having to provide an username) or to identify the user (the user provides only the fingerprint and the application decides to whom this characteristic belongs to; this is a 1:n comparison and is not quite suitable for internet banking authentication, because of the possible big number of user enrolled).

V. CONCLUSIONS

As we could see, biometric characteristics are suitable to be used in internet banking applications in order to increase the security. The user has to provide a biometric characteristic, but also the system must be adaptable in order to accept only that biometrics that user can provide. A physical impairment in a non-adaptive system will lead to the impossibility to use the application. Many other applications and researches can be developed in order to increase the security in such a sensitive domain like internet banking.

VI. ACKNOWLEDGMENT

This paper was supported by the project "Sustainable performance in doctoral and post-doctoral research - PERFORM - Contract no. POSDRU/159/1.5/S/138963", project co-funded from European Social Fund through Sectoral Operational Program Human Resources Development 2007-2013.

VII. REFERENCES

[1] C., Lupu, V.G., Găitan, V. Lupu, *"Security enhancement of internet banking applications by using multimodal biometrics"*, IEEE 13th International Symposyum on Applied Machine Intelligence and Informatics (SAMI 2015), Jan. 22-24, 2015, Herl'any, Slovakia, pp. 47-52, ISBN 978-1-4799-8220-2, 978-1-4799-8221-9, available online at: http://www.uni-obuda.hu/users/szakala/SAMI2015%20pendrive/9_sami2015.pdf (last accessed: Jan. 15, 2015)

[2] C. Lupu, V. Lupu, *"The beginnings of using fingerprints as biometric characteristics for personal identfication purposes"*, Annals of the „Constantin Brancusi" University of Targu Jiu, Engineering Series, No. 3/2014, pp. 53-56, ISSN 1842-4856, available online at: http://www.utgjiu.ro/revista/ing/pdf/2014-3/8_Catalin%20Lupu.pdf (last accessed on Jan. 15, 2015)

[3] C. Lupu, V. Lupu, *"Biometrics used for authentication in internet-banking applications"*, Annals of the „Constantin Brancusi" University of Targu Jiu, Engineering Series, No. 3/2014, pp. 57-63, ISSN 1842-4856, available online at: http://www.utgjiu.ro/revista/ing/ pdf/2014-3/9_Catalin%20Lupu.pdf (last accessed on Jan. 15, 2015)

[4] C. Lupu, "*Development of optimal filters obtained through convolution methods, used for fingerprint image enhancement and restoration*", "The USV annals of Economics and Public Administration", Volume 14, issue 2(20), 2014, pp. 156-167, ISSN 2285–3332 (printed), 2344–3847 (online)

[5] S.S. Hoseini and S. Mohammadi, *"Review banking on biometric in the world's banks and introducing a biometric model for Iran's banking system"*, Journal of Basic and Applied Scientific Research, Part III 2(9), September 2012, pp. 9152-9160, available online at http://www.textroad.com/Old%20Version/pdf/JBASR/J.%20Basic.%20Appl.%20Sci.%20Res.,%202(9)9152-9160,%202012.pdf (last accessed on Jan. 15, 2015)

[6] *Ross, K. Nandakumar, A.K. Jain, "Handbook of multibiometrics", Springer, 2006, ISBN 978-0-387-22296-7*

[7] J.L. Wayman, A.K. Jain, D. Maltoni, D. Maio, "*Biometric systems: technology, design and performance evaluation*", Springer, 2005, ISBN 978-1-84628-064-1

[8] F. Galton, "*Finger Prints*", MacMillan and Co., 1892, available online at http://galton.org/books/ finger-prints/index.htm (last accessed on Jan. 15, 2015)

[9] G. Pasescu, I.R. Constantin, "*Secretele amprentelor papilare*", Editura National, 1996, ISBN 973-97574-0-5

[10] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, "*Handbook of fingerprint recognition*", Springer,2005, ISBN 0-387-95431-7

[11] L. Flom, A. Safir, "*Iris recognition system",* United States Patent no. 4.641.349, 1987, available online at: https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US4641349.pdf (last accessed on Jan. 15, 2015)

[12] J. Daugman, "*Biometric personal identification system based on iris analysis*", US Patent no. 5.291.560, 1994, available online at: https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US5291560.pdf (last accessed on Jan. 15, 2015)

[13] J. Daugman, "*How iris recognition works*", IEEE Transactions on circuits and systems for video technology, Vol. 14, no. 1, pp. 21-30, ISSN 1051-8215, available online at: http://www.cl.cam.ac.uk/~jgd1000/csvt.pdf (last accessed on Jan. 15, 2015)

[14] Moldoveanu, F., "Tehnici de imbunatatire si restaurare a imaginilor", Bucuresti 2013

[15] Canny, J., "*A computational approach to edge detection"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, PAMI-8(6):679–698, Nov. 1986.

[16] Moeslund, T.B., "*Image and Video Processing*", August 2008

[17] Green, B., "*Canny edge detection tutorial"*, http://dasl.mem.drexel.edu/alumni/bGreen/www.pages.drexel.edu/_weg22/can_tut.html (last accessed: Jan. 15, 2015)

[18] M. Burge, K. Boweyer, *"Handbook of iris recognition",* Springer, 2013, ISBN 978-1-4471-4401-4

Eng. **Cătălin LUPU** graduated in 2003 the Electrical Engineering Faculty, Computer Science Department, from „Ştefan cel Mare" University of Suceava. In 2013, he became a Ph.D. student at „Ştefan cel Mare" University of Suceava, , at professor Ph.D. eng. Vasile-Gheorghiță Găitan. The Ph.D. thesis is called „Personal recognition using fingerprint and iris". For two years (2004-2006) he was an associated assistant at „Ştefan cel Mare" University of Suceava, Faculty of Economic Science and Public Administration, Informatics Department. He published many articles in national and international conference proceedings.

Prof. Ph.D. eng. **Vasile-Gheorghiță GĂITAN** is a professor at "Ştefan cel Mare University" of Suceava, Faculty of Electrical Engineering and Computer Science since 1990. He obtained the professor degree in 2004. He is a specialist in microcontrollers, microprocessors and local industrial networks. In these domains, he published many articles in national and international journals.

Prof. Ph.D. **Valeriu LUPU** is a professor at "Ştefan cel Mare University" of Suceava, Faculty of Economics and Public Sciences, Informatics board since 1990. He obtained the professor degree in 2009. He is a specialist in databases, web technologies and programming languages, having published 8 books and many articles in national or international journals.