ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 2012. No. 5(121)
ELEKTRONIKA IR ELEKTROTECHNIKA

SYSTEM ENGINEERING, COMPUTER TECHNOLOGY
T 120
SISTEMŲ INŽINERIJA, KOMPIUTERINĖS TECHNOLOGIJOS

Study of Finger Vein Authentication Algorithms for Physical Access Control

A. Venckauskas, N. Morkevicius
Computer Department, Kaunas University of Technology,
Studentų str. 50, LT-51368, Kaunas, Lithuania, phone: +370 37 300386,
e-mails: algimantas.venckauskas@ktu.lt, nerijus.morkevicius@ktu.lt
K. Kulikauskas
Synthesis Inc.,
318 72nd St., Brooklyn, New York, USA, e-mail: kristijonaskulikauskas@yahoo.com

crossref http://dx.doi.org/10.5755/j01.eee.121.5.1660

Introduction

The purpose of any physical security system is to permit only authorized users to access restricted objects/areas. There are various examples of physical security: territory, room, automobile, etc. Physical security appliances operate in complex conditions: rain, temperature fluctuations, dust, dirt, etc. Users of security systems encompass a vast range of people; they can be old or young and have varying degrees of ability to operate such systems. Security systems must be able to both control access to objects/areas and also to save and contain data relevant to the access of these objects/areas. Therefore, these systems have to be smart, reliable (unbreakable), simple to use, resistant to environmental impacts and cheap (not requiring a lot of resources).

Biometric authentication methods for access control

Various user authentication methods are used in contemporary electronic security systems [1, 2]: certain codes – password, personal identification number (PIN); electronic cards – magnetic, smart-cards; biometrical methods – physical user parameters: fingerprint, face, hand shape, eye iris, vein image; behaviour: voice, writing. Systems that operate by using passwords or PIN numbers require the individual to memorize the code. However, such systems cannot determine the person who enters it. Systems that use cards for access control only determine card authenticity, but not the authenticity of the person who presents it. Therefore, systems based on code and card usage cannot ensure high object security. Various biotronic measures are used in contemporary electronic systems [3]. Biometric devices verify who a person is by what they are, whether it is their hand, eye, fingerprint or voice [4, 21]. Biometrics can also eliminate the need for cards. Growth of the biometric industry also highlights the prospect of biometric systems: the market for biometric core technology will increase from $2,584 billion in 2009, to $10,882 billion in 2017, a forecasted yearly growth of 19.69% [5]. Biometrics will be a fundamental embedded component of the digital world, as it becomes a key enabler of trusted transaction control – data access and flow - for personal, commercial and government use.

Distribution of biometrical technologies is shown in Fig. 1 [6].

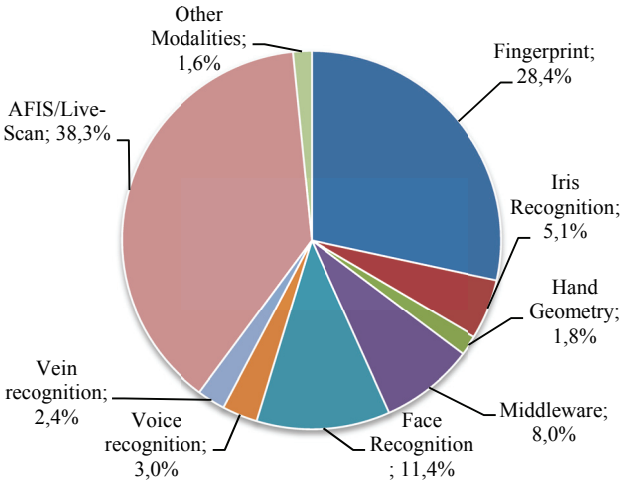

Fig. 1. Biometric Revenues by Technology, 2009 (© 2008 International Biometric Group)

Finger vein authentication thus offers considerably more advantages compared to other forms of biometrics. These comparative advantages are collectively shown in Table 1 [7].

Table 1. Comparison of major biometrics methods

BIOMETRICS	SECURITY		CONVENIENCE				
	Anti-Forgery	Accuracy	Speed	Enrollment rates	Resis-tance	Cost	Size
Fingerprint	⊗	O	O	⊗	⊗	⊕	⊕
Iris	O	⊕	O	O	⊗	⊗	⊗
Face	O	⊗	O	O	⊕	⊗	⊗
Voice	O	⊗	O	O	⊕	O	O
Vein Pattern	⊕	⊕	⊕	O	O	O	O

Note: ⊕: good, O: normal, ⊗: insufficient

The Riley's et al. evaluation [8] suggests that vein technology is more accessible for an older population using than fingerprint technology. Using fingerprint based technologies for physical access is problematic for the following reasons: environmental conditions (dust, dirt, temperature fluctuation), fingerprint image quality is low, they can be forged and it can be more complicated for the elderly.

The finger vein pattern based authentication method is highly reliable, the veins are hidden underneath the skin's surface so forgery is extremely difficult; it is non-invasive and easy to use, offering a balance of advantages. These unique aspects of finger vein pattern recognition set it apart from previous forms of biometrics [7].

Let's examine finger vein pattern usage problems. A finger vein image is obtained using an infrared scanner, so its quality, depending on environment can be erratic and sometimes poor. Quality parameters of authentication system, false acceptance and false rejection [9], highly depend on finger vein image processing algorithms and their resistance to noise i.e. image quality.

Important issues for biometric systems are research of efficiency [10]. NIST performed comprehensive analysis of fingerprint solutions (technologies) [11]. Eighteen different companies competed, and 34 systems were evaluated. There is a lack of finger vein based technology analysis.

Finger vein recognition algorithm

Finger vein recognition – a relatively embryonic field, new methods are developed and existing ones are examined. Miura et al. proposed a method of extracting finger vein patterns by using repeated line tracking from various starting positions [12]. Zhang et al. proposed an extraction method based on curve let information of the profile of finger vein images and locally interconnected structured neural networks [13]. Mahri et al. proposed an algorithm for finger vein recognition with less complexity in the image preprocessing phase, where finger vein pattern extraction is not included at all. In the proposed algorithm, they implement a phase-only correlation function at the matching stage with a very simple preprocessing technique [14]. All of the previously described methods use the features from the extracted vein patterns for recognition. However, finger vein images are not always clear and can show irregular shadings and highly saturated regions. Therefore, detection errors can occur when extracting accurate vein patterns.

Well-developed fingerprint recognition methods have been used for many years [15, 16, 17 and 18]. Further, we will research fingerprint recognition method suitability for finger vein recognition. We will study three algorithms. Abraham et al. proposed a method for fingerprint matching using a hybrid shape and orientation descriptor (Algorithm A1) [16]. Jain et al. proposed filter-based algorithm, that uses a bank of Gabor filters to capture both local and global details in a fingerprint as a compact fixed length FingerCode (Algorithm A2) [17]. Ng et al. analyzed a novel fingerprint feature named adjacent orientation vector for fingerprint matching (Algorithm A3) [18].

Experiments

During the experiment we explored fingerprint recognition method suitability for finger vein recognition as well as how image resolution and noise influences results. We used images from the experiment of Intelligent Biometric Group [19]. In order to imitate different finger vein scans, we altered the hue, contrast and brightness of images with image editing software, so that we obtained 5 images of each finger. To imitate environment influence such as dirt or the illumination of surroundings, we added different levels of noise with image editing software, using Perlin noise function [20], respectively: level 1 - 0%, level 2 - 5%, level 3 - 10% and level 4 - 20%. To imitate different resolutions of a CCD camera, we used series of different resolution images for the experiment: level 1 - 180 x 60 pixels, level 2 - 150 x 50 pixels, level 3 - 120 x 40 pixels, level 4 – 90 x 30 pixels. By using these methods we had 16 series, each made up of 20 images. Researched finger vein image examples are presented in Fig. 2–Fig. 4.

Fig. 2. Unmodified image with original resolution

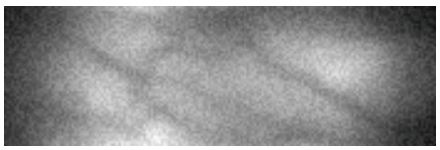

Fig. 3. Original resolution image with added noise

Fig. 4. Lowest resolution image with added noise

Simulation was performed in Matlab 2007b environment, using three algorithms – A1, A2 and A3.

Experiment- we compared each image from all series with remaining same series images and recorded the results: true acceptance, false rejection and false acceptance. Results are presented in Table 2.

The true acceptance rate's dependence on different resolution, using different algorithms without Perlin noise are presented in Fig. 5. As we can see, we get the most stable results from Algorithm A1.

Table 2. Results of finger vein recognition algorithm research

Resolution Level	Perlin Noise Level	Algorithm A1			Algorithm A2			Algorithm A3		
		True Acceptance Rate, %	False Rejection Rate, %	False Acceptance Rate, %	True Acceptance Rate, %	False Rejection Rate, %	False Acceptance Rate, %	True Acceptance Rate, %	False Rejection Rate, %	False Acceptance Rate, %
1	1	98	0	2	90	10	0	100	0	0
1	2	91	7	2	55	40	5	100	0	0
1	3	58	40	2	5	90	5	100	0	0
1	4	56	44	0	0	100	0	100	0	0
2	1	91	9	0	90	10	0	95	5	0
2	2	84	16	0	70	25	5	95	5	0
2	3	81	16	3	35	55	10	85	15	0
2	4	79	21	0	5	90	5	75	15	10
3	1	92	7	1	87	13	0	83	17	0
3	2	91	7	2	76	18	6	82	18	0
3	3	87	12	1	69	23	8	70	30	0
3	4	86	14	0	62	38	0	53	35	12
4	1	93	7	0	85	15	0	60	40	0
4	2	95	0	5	95	5	0	60	40	0
4	3	86	9	5	90	10	0	60	40	0
4	4	94	5	1	95	5	0	40	40	20

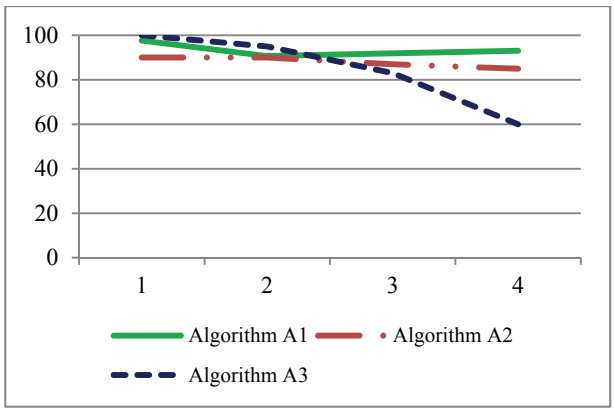

Fig. 5. True acceptance rate's dependence on different resolution using different algorithms

The true acceptance rate's dependence on Perlin noise level, using different algorithms with resolution level 1 are presented in Fig. 6. As we can seem we get the most stable results from algorithm A3.

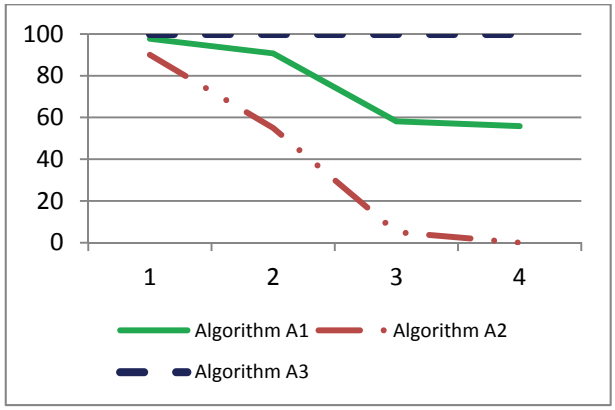

Fig. 6. True acceptance rate's dependence on Perlin noise, using different algorithms

Table 3. Overall algorithm assessment

	Algorithm		
	A1	A2	A3
Resolution			
True Acceptance	3	3	2
False Rejection	2	1	3
False Acceptance	2	3	1
Amount	7	7	6
Perlin Noise			
True Acceptance	3	1	3
False Rejection	2	1	2
False Acceptance	3	1	2
Amount	8	3	7
Total	**15**	**10**	**13**

We summarized our results in a table, assessing results of algorithms: 3 – good, 2 – average, 1 – poor (Table 3), using level 4 resolution and level 4 Perlin noise. It is clear that in the conditions of our experiment we get the best results from algorithm A1.

As we can see from Table 3, when image resolution is decreasing and noise is increasing, we get the best results from algorithm A1 - method for fingerprint matching using a hybrid shape and orientation descriptor. Using primary image resolution and all noise levels, we get best results from algorithm A3. Algorithm A2 is very sensitive to noise and as it increases, false acceptance rate highly increases.

Conclusions

Biometrical access control methods are increasingly being used in physical security systems. Finger vein authentication methods appear promising for the future when assessing reliability and user-friendliness.

In this study, we researched the possibilities of using fingerprint recognition methods for finger vein recognition.

Experiments showed that the method for fingerprint matching using a hybrid shape and orientation descriptor from these researched algorithms for physical access systems suits most.

This method is least sensitive to finger vein image quality – the true acceptance rate is 98% with primary quality and it only drops to 56% with the worst quality. Such indicators satisfy practical extreme conditions.

References

1. **Anderson Ross J.** Security Engineering: A Guide to Building Dependable Distributed Systems. – John Wiley and Sons, 2010. – 1080 p.
2. **O'Gorman L.** Comparing passwords, tokens, and biometrics for user authentication // Proceedings of the IEEE, 2003. – Vol. 91. – No. 12. – P. 2019–2040.
3. **Balaišis P., Eidukas D., Keras E., Valinevičius A.** The Selection of Biotronics Measures // Electronics and Electrical Engineering. – Kaunas: Technologija, 2010. – No. 1(97). – P. 9–14.
4. **Ivanovas E., Navakauskas D.**. Development of Biometric Systems for Person Recognition: Biometric Feature Systems, Traits and Acquisition // Electronics and Electrical Engineering. – Kaunas: Technologija, 2010. – No. 5(101). – P. 87–90.
5. **Acuity Market Intelligence.** The Future of Biometrics. Market Analysis, Segmentation & Forecasts. Insights into the Trends, Drivers & Opportunities that will Shape the Industry through 2020. – 2009. Online: http://www.acuity–mi.com/Future_of_Biometrics.html.
6. **International Biometric Group.** Biometrics Market and Industry Report 2009–2014, December 2009. // http://www.ibgweb.com/products/reports/bmir–2009–2014.
7. **Hashimoto J.** Finger Vein Authentication Technology and Its Future // VLSI Circuits, 2006. – Digest of Technical Papers. – P. 5–8.
8. **Riley C., McCracken H., Buckner K.** Fingers, veins and the grey pound: accessibility of biometric technology // Proceedings of the 14th European conference on Cognitive ergonomics (ECCE'07). – New York, NY, USA, 2007. – P. 149–152.
9. **Jain A. K., Pankanti S., Prabhakar S., Lin Hong, Ross A.** Biometrics: a grand challenge // Proceedings of the 17th International Conference (ICPR'2004), 2004. – Vol. 2. – P. 935–942.
10. **Balaišis P, Gužauskas R., Eidukas D., Valinevičius A.** Directions of Efficiency Research for Biotronics Technologies // Electronics and Electrical Engineering. – Kaunas: Technologija, 2009. – No. 1(89). – P. 49–54.
11. **Wilson C., Hicklin R. A., Korves H., et al.** Finger–print Vendor Technology Evaluation 2003. – Summary of Results and Analysis Report, NIST Research Report: 7123, 2004.
12. **Miura N., Nagasaka A., Miyatake T.** Feature extraction of finger–vein patterns based on repeated line tracking and its application to personal identification // Machine Vision and Applications, 2004. – Vol. 15. – No. 4. – P. 194–203.
13. **Zhang Z., Ma S., Han X.** Multiscale Feature Extraction of Finger–Vein Patterns Based on Curvelets and Local Interconnection Structure Neural Network // Pattern Recognition, 2006. – 18th International Conference ICPR'2006. – Vol. 4. – P. 145–148.
14. **Mahri N., Suandi S. A. S., Rosdi B. A.** Finger Vein Recognition Algorithm Using Phase Only Correlation // Emerging Techniques and Challenges for Hand–Based Biometrics (ETCHB), 2010. – P. 1–6.
15. **Kisel A., Kochetkov A., Kranauskas J.** Fingerprint Minutiae Matching without Global Alignment Using Local Structures // Informatica, 2008. – Vol. 19. – No. 1. – P. 31–44.
16. **Abraham J., Kwan P., Junbin Gao.** Fingerprint Matching using A Hybrid Shape and Orientation Descriptor // InTech, 2011. – P. 25–56.
17. **Jain A. K., Prabhakar S., Hong L., Pankanti S.** Filterbank–based fingerprint matching // Image Processing, IEEE Transactions, 2000. – Vol. 9. – No. 5. – P. 846–859.
18. **Ng G. S., Tong X., Tang X., Shi D.** Adjacent orientation vector based fingerprint minutiae matching system // Pattern Recognition, 2004. – Proceedings of the 17th International Conference ICPR'2004. – Vol. 1. – P. 528–531.
19. **USM–IBG.** Finger vein biometric system. Online: http://ibg–usm.org.
20. **Perlin K.** Improving noise // ACM Transactions on Graphics (TOG), 2002. – Proceedings of ACM SIGGRAPH'2002. – Vol. 21. – Iss. 3. – San Antonio, Texas, 2002. – P. 681–682.
21. **Wang F., Han J.** Robust Multimodal Biometric Authentication Integrating Iris, Face and Palmprint // Information Technology And Control. – Kaunas: Technologija, 2008. – Vol. 37. – No. 4. – P. 326–332.

Received 2012 01 21
Accepted after revision 2012 03 19

A. Venckauskas, N. Morkevicius, K. Kulikauskas. Study of Finger Vein Authentication Algorithms for Physical Access Control // Electronics and Electrical Engineering. – Kaunas: Technologija, 2012. – No. 5(121). – P. 101–104.

In this study problems of using biometric authentication methods for physical access systems are analyzed. Possibilities for applying biometric authentication methods are also examined. It is suggested that fingerprint recognition methods could be applied to finger vein recognition. The experiment shows that method for fingerprint matching using hybrid shape and orientation descriptor finger vein recognition could be used in finger vein based physical access systems. Finger vein image quality has low impact for this method. Ill. 6, bibl. 21, tabl. 3 (in English; abstracts in English and Lithuanian).

A. Venčkauskas, N. Morkevičius, K. Kulikauskas. Pirštų kraujagyslių tapatumo nustatymo algoritmų taikymo fizinės apsaugos sistemose tyrimas // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2012. – Nr. 5(121). – P. 101–104.

Darbe sprendžiamos biometrinių tapatumo nustatymo metodų taikymo fizinės apsaugos sistemose problemos. Išnagrinėtos biometrinių tapatumo nustatymo metodų taikymo galimybės. Pasiūlyta pirštų atspaudų atpažinimo metodus pritaikyti pirštų kraujagyslėms atpažinti. Eksperimentiškai parodyta, kad pirštų kraujagyslėms atpažinti fizinės saugos sistemose galima taikyti figūros konteksto ir orientacijos deskriptoriais atvaizdų atpažinimo principu veikiantį metodą. Šis metodas nelabai jautrus kraujagyslių atspaudų kokybei. Il. 6, bibl. 21, lent. 3 (anglų kalba; santraukos anglų ir lietuvių k.).