computing@tanet.edu.te.ua
www.computingonline.net

ISSN 1727-6209
International Journal
of Computing

USER AUTHENTICATION BASED ON BEHAVIORAL PATTERNS

Adrian Kapczyński [1], Paweł Kasprowski [2], Piotr Kuźniacki [3]

[1] Silesian University of Technology, adrian.kapczynski@polsl.pl, www.biometrics.pl
[2] Silesian University of Technology, pawel.kasprowski @polsl.pl, www.kasprowski.pl
[3] Silesian University of Technology, piotr.kuzniacki@polsl.pl, www.kuzniacki.net

Abstract: *In this paper biometric techniques based on eye movement and keystroke dynamics were examined. In the first part theoretical aspects concerning biometrics were presented. In second part two prototype systems were characterized: first based on eye movement dynamics and the second based on keystroke dynamics. In the third part chosen system was taken into testing which quantitative effects were presented in categories of FRR, FAR and HTER indicators.*

Keywords: *Security, biometrics, behavioral biometrics, eye movement analysis, OBER system, keystroke dynamics.*

1. INTRODUCTION

After analysis of state-of-the art [1, 2, 11] it can be stated that key focus in research in area of biometric methods is set on methods based of anatomy of given part of human body (e.g. iris, retina, fingerprint). It has been found that the other group of biometric methods, based on analysis of characteristics of behavioral patterns, is emerging and requires in-depth analysis.

The key point of this article is to present the current state-of-the-art of research carried out by authors in this domain which enables formulation of fundamental basis for further development.

In the first part of the article the biometrics preliminaries was presented and it the second part two developed methods were characterized and one them was put into examination.

2. BIOMETRICS PRELIMINARIES

One of the most dangerous security threats is the impersonation and the security services that encounter this threat is verification and identification.

During identification identity is assigned to a specific individual (one-to-many comparisons) and verification is designed to verify a identity of given user (one-to-one comparison). The verifier can be identified or verified by what he knows (e.g. password), by what he owns (e.g. token) or by anatomical or behavioral characteristics. Biometric systems verify or identify a person by examining his physical features or behaviors. The first group of methods measures the physiological characteristics of a person (e.g. fingerprint, iris, ear shape and others). The latter group, i.e. based on behavioral characteristics, measures the behavior of a man (e.g. signature, keystroke dynamics, etc.).

Authentication systems are functioning mainly in verification mode [2]. This means that every user in order to be capable of being verified by the system shall successfully finish the enrolment (biometric characteristics acquisition), next transformed into feature vector and finally stored as biometric template in a database (Fig. 1).

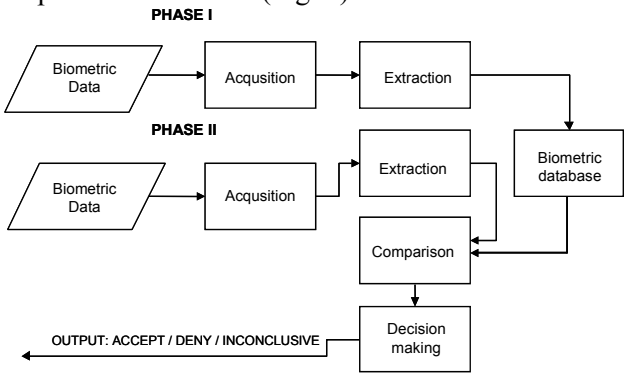

Fig. 1. Biometric authentication system

One shall assume that the whole population of users divides into genuine users and impostors. The impostors are making false attempts, i.e. try to be successfully verified by claiming to be someone else. The genuine users are making true attempts – they intentions are opposite to impostors' ones. During the verification the reference biometric template stored in database is compared with verification template acquired from the user. The

result of the comparison is a confidence degree (e.g. expressed in percent) which is confronted with threshold value. If confidence degree is equal or greater than threshold value than the system accepts the attempt otherwise produces decision deny [11].

In order to properly present and analyze the anatomy of biometric authentication systems, a new easy-in-use methodology was needed. The only one that has appeared and has met the requirements was created by J. Ashbourn and named BANTAM – Biometric and Token Application Modeling Language [1]. A model of classical biometric authentication system was presented on Fig. 2.

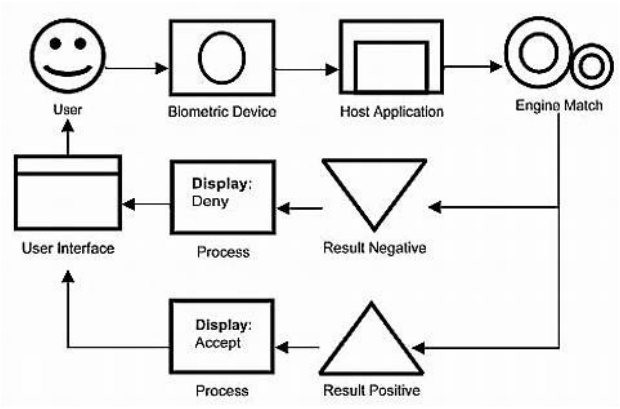

Fig. 2. Model of biometric authentication system (example of use of BANTAM language)

In the empirical part of this article two biometric methods based on behavioral patterns were characterized.

3. EYE MOVEMENT BIOMETRICS

Eyes are one of the most important human organs. Therefore, it is not a surprise that using eyes to perform human identification in biometric methods has a long tradition including well established iris pattern recognition algorithms [3] or retina scanning. But these techniques measure only physiological parameters of eyes. Identifying people by the way they are using their eyes may be more interesting.

Eyes are the main 'interface' between environment and human brain and the system which deals with human vision is physiologically and neurologically complicated. To enable brain to acquire image in real time, the system which controls eye movements (termed oculomotor system) has to be very fast and accurate. It is built of six extra ocular muscles which act as three agonist/antagonist pairs concerned with horizontal, vertical and oblique rotations of eye [4]. Eyes are controlled directly by the brain with three cranial nerves originating from midbrain and pons. Therefore its movements are the fastest reactions for changing environment (Fig. 3).

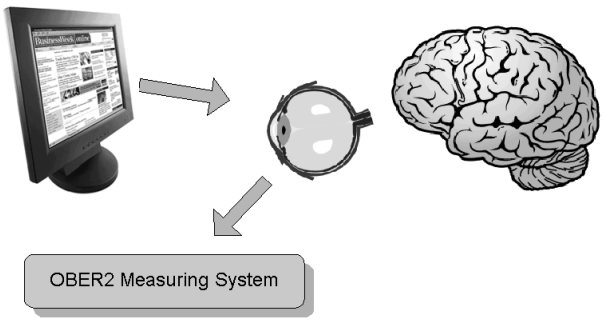

Fig. 3. The idea of eye movement biometric system

When individual looks at an object, the image of the object is projected on to the retina, which is composed of light-sensitive cells that convert light into signals which in turn can be transmitted to brain via the optic nerve. The density of these light-sensitive cells on retina is uneven, with denser clustering at the centre of the retina rather than at the periphery. Such clustering causes the acuity of vision to vary, with the most detailed vision available when the object of interest falls on the centre of the retina. This area is called yellow dot or fovea and covers about two degrees of visual angle. Outside this region visual acuity rapidly decreases. Eye movements are made to reorient the eye so that the object of interest falls upon the fovea and the highest level of detail can be extracted [5].

That is why it is possible to define a 'gaze point' – an exact point a person is looking at in a given moment of time. When eyes are looking at something for a period of time this state of the eye is called a fixation. During that time the image which is projected on the fovea is analyzed by the brain. The standard fixation lasts for about 200-300 ms, but of course it depends on the complexity of an image which is observed. After the fixation, eyes move rapidly to another gaze point – another fixation. This rapid movement is termed a saccade. Saccades differ in longitude, yet always are very fast (Fig. 4).

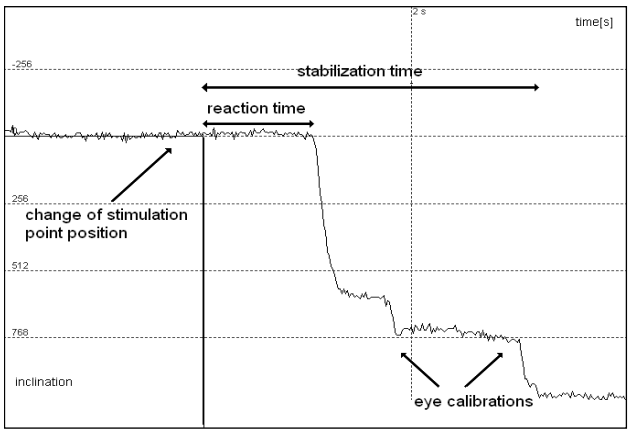

Fig. 4. Example of eye movement reaction for stimulation point (in one axis)

Eye movements may give a lot of information

about an individual. The way the gaze point is moving through the image is often the result of person's previous experience [6]. The experiment described in this paper used a 'jumping point' stimulation to observe person's reactions. It that kind of stimulation the screen is blank with only one point 'jumping' through it. The task of examined persons is to follow the point with their eyes. There are nine different point placements defined on the screen, one in the middle and eight on the edges, creating 3 x 3 matrix. The point flashes in one placement in a given moment. The stimulation begins and ends with a point in the middle of the screen. During the stimulation, point's placement changes in specified intervals (Fig. 5).

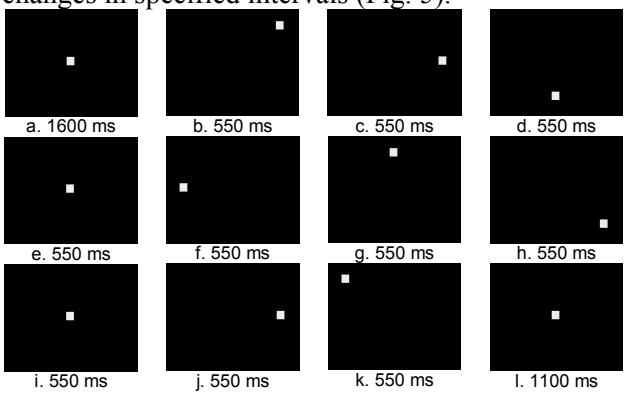

Fig. 5. Example of eye movement reaction for stimulation point (in one axis)

Implemented system was evaluated – the results were presented in chapter 5.

4. KEYSTROKE BIOMETRICS

Keystroke dynamics is a behavioral biometric technique based on analysis of characteristics of individual way that a user interacts with a computer keyboard. Keyboard characteristics are rich in cognitive qualities and experiments for keystroke characterization showed high degree of correlation when the same person typed both reference keystroke and the test ones. The first intentional use of keystroke dynamics for person identification was in 1975 [12]. Since then it is generally approved that keystroke biometrics measure typing characteristics are unique to individual person and thus difficult to duplicate [13]. Keystroke biometrics hold great promise to become standard method of user authentication. It's very inexpensive method without the need of any special hardware and has an advantage over other biometrics methods – acceptance of users. Because using login and password to authenticate is obvious for most users and because of the fact, that keystroke dynamics may depend on these phrases, this technology could be almost completely transparent.

Analyzing keystroke dynamics is a process that analyzes the way users type by monitoring the keyboard inputs and then identifies users on their individual typing rhythm patterns. While the user is typing a string key down and up times are captured to achieve features: duration of the key and keystroke latency. Duration of the key is the time that a key remains pressed (time interval between pressing and releasing the key) and keystroke latency is the time between two keystrokes (Fig. 6).

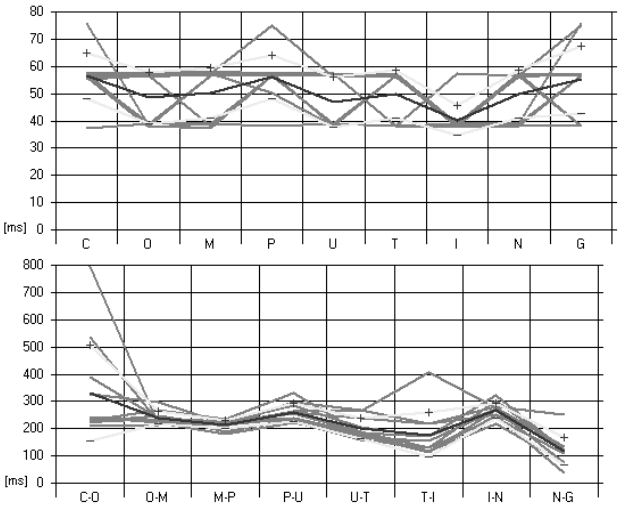

Fig. 6. Mean and variance of duration of the key and keystroke latency in fixed string "computing"

The main problem with measuring the time of pressing and releasing keys is timing accuracy. The results depend on the keyboard type, hardware, OS version and computer configuration. Transfer of signal identifying a keypress from the keyboard to program can have large variability. Our novel approach is to focus on this problem, which is not considered in other related works.

The first aim to resolve the problem is to understand how keyboard, keyboard controller and software layer works in PCs. The keyboard is nowadays the primary input device for software on the PC system, so learning how it works is very important. Every keyboard has inside microcontroller chip that constantly scans a large matrix of keys to determine if any keys are down. To get rid of phenomenon known as keybounce, when contacts bounce off one another many times before coming to rest making a clean contact during a keypress, controller has a special scan algorithm, that employs delays while scanning keys. Therefore there is first place where some delay could be noticed. After capturing pressing or releasing key keyboard controller sent appropriate coded data to the host through serial communication channel according to IBM protocol. Computer also contains controller that is in charge of decoding all of the data received from keyboard controller and then they are

processed by the keyboard's interrupt service routine. There are several methods how to receive pressed keys in operating system. In Microsoft Windows it can be achieve through: simple key events in application, hook mechanism, DirectX access or keyboard driver.

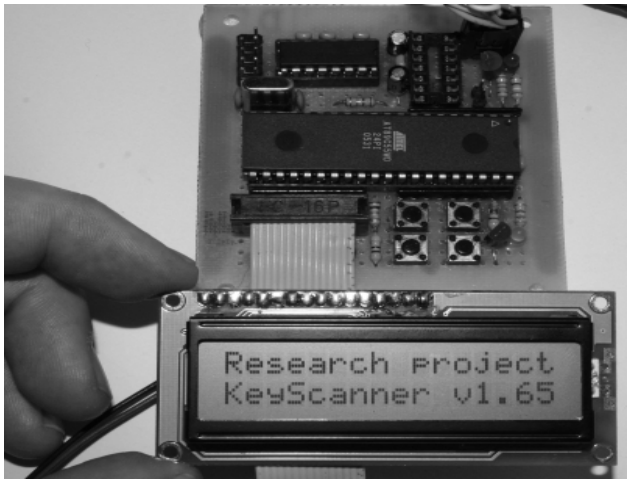

Fig. 7. Designed device KeyScanner

To determine how big influence has a type of mainboard chipset, computer configuration and chosen level of intercepting pressed keys in operating system it would be necessary to type on keyboard each time exactly in the same way. It cannot be done by human, but it is possible for special device.

We designed device named KeyScanner (Fig. 7) which can be plugged in between keyboard and computer and therefore can listen all communication between keyboard controller and host controller.

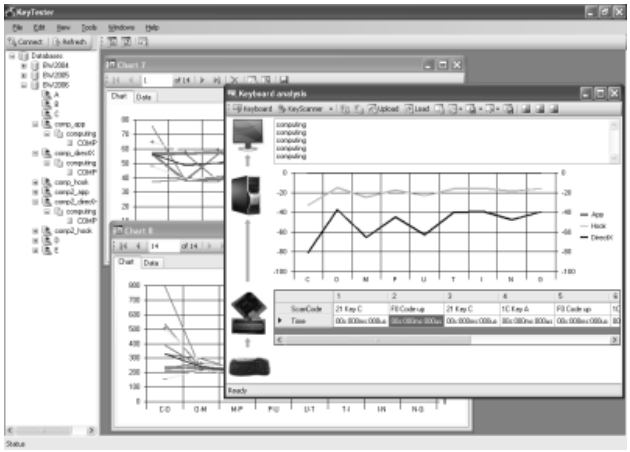

Fig. 8. Research environment KeyTester

It is possible to track each pressed key on keyboard with KeyScanner and mark exactly time of press and release of key in microseconds. Device can also save typed text and repeat according keystrokes for several times. To perform planed researches we create also complex environment (Fig. 8) that allows realizing different research scenario. According to currently researches, results indicate that proper method of collecting received pressed keys and time may be fundamental – distinctions of measured time could be in milliseconds when the computer is overloaded during identification process.

5. EVALUATION

During evaluation 47 persons at the age ranging from 19 to 38, both males and females were taken into account. There were overall 1151 experiments performed. Each experiment result was than transformed using several universal and subject specific transformations (like wavelets, eye distance etc.). The described experiment produced a lot of data which was than analyzed in EyeStat application [7]. The results of errors calculations were then averaged giving values presented in Table 1. On Fig. 9 the "worse", "average" and "best" results were presented. Abbreviation FAR stands for False Acceptance Rate, abbreviation FRR stands for False Rejection Rate and Half Total Error Rate (HTER) is the average of both of them.

Table 1. Average error rates [%]

FAR	FRR	HTER
4,84	9,40	7,12

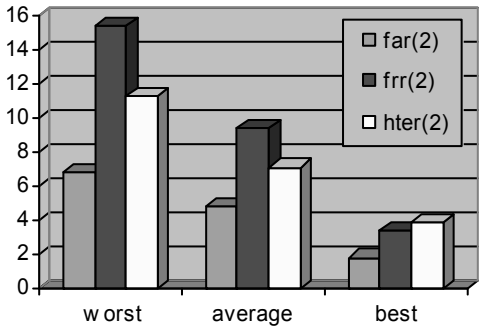

Fig. 9. Results of examination of eye movement biometric system (errors rates in %)

Quantitative results obtained during examination of biometric authentication system based on behavioral pattern, i.e. eye movement are quite interesting and motivating to continue the research work in this area.

6. CONCLUSIONS

In the article two chosen biometric methods were taken into in-depth analysis: keystroke biometrics, and eye movement biometrics.

The advantages of keystroke dynamics in user authentication are quite obvious. Assuming that the input device is the existing keyboard, this technology is only a cost of software and could be a

standard in short time without many problems hinder other biometrics technologies. Differences in the physical characteristics of keyboards should be in special consideration in subsequent works. Measuring the time must be done as near keyboard device as possible to correctly track each pressed key and mark exactly time of press and release of key. Therefore keystroke dynamics could also come in the form of a built-in hardware in keyboards or motherboard, not only software [14].

The idea of personal identification using eye movement characteristic seems to be valuable addition to other well known biometric techniques [8, 9]. What makes it interesting is the easiness of combining it with, for instance, face or iris recognition. As all of those techniques need digital cameras to collect data, the system that uses the same recording devices to gather information about human face shape, eye iris pattern and eye movements characteristic may be developed. Of course there is a lot of work to be done to improve the methodology, but first experiments show the great potential of eye movements identification.

Further research works include implementations of described methods in real-life applications, including internet identification for purposes of e-learning and e-commerce solutions.

7. REFERENCES

[1] J.Ashbourn: *BANTAM*. Springer Verlag. London, 2002

[2] J. Ashbourn: *Biometrics – advanced identity verification*. Springer Verlag. London, 2000

[3] J. Daugman,: High Confidence Visual Recognition of Persons by a Test of Statistical Independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, 1993

[4] G. K. Hung: Models of Oculomotor Control, World Scientific Publishing Co., 2001

[5] L. Cowen, L.J. Ball, J.Delin: An eye-movement analysis of web-page usability. Chapter in X. Faulkner, J. Finlay, & F. Détienne (Eds.): *People and Computers XVI—Memorable Yet Invisible: Proceedings of HCI 2002*. Springer Verlag. London, 2002

[6] D. Noton, L. Stark: Scanpaths in eye movements during pattern perception. Science, 171, 1971

[7] P. Kasprowski. Human Identification Using Eye Movements. Ph.D. Thesis. Silesian University of Technology. Gliwice, 2004

[8] P. Kasprowski, J. Ober. With the flick of an eye, Biometrics Technology Today ISSN 0969-4765, Volume 12, Issue 3, Elsevier Science (2004)

[9] P. Kasprowski, J. Ober. Eye Movement in Biometrics. *Proceedings of Biometric Authentication Workshop, European Conference on Computer Vision in Prague 2004*. Springer Verlag. London, 2004

[10] A. Kapczyński. About implementation of multiple biometrics authentication system. *Proceedings of 2nd International Conference on Information and communication technology security*. WSiIZ. Bielsko-Biała, 2003

[11] S. Nanavanti, M. Thieme, R. Nanavati. Biometrics - identity verification. Wiley & Sons, Inc. NY, 2002

[12] R. Spillane. Keyboard Apparatus for Personal Identification. *IBM Technical Disclosure Bulletin* vol. 17, no. 3346, 1975

[13] J. Leggett. Dynamic Identity Verification via Keystroke Characteristics, Int'l J. Man-Machine Studies, vol. 35, no. 6, 1991

[14] F. Monrose, A. Rubin. Keystroke Dynamics as a Biometric for Authentication. Future Generations Computing Systems, vol. 16, no. 4, 2000, pp. 351–359

[15] R. Gaines. Authentication by Keystroke Timing: Some Preliminary Results, tech. report R-256-NSF, RAND, 1980

[16] R. Joyce, G. Gupta. Identity Authentication Based on Keystroke Latencies. Comm. ACM, vol. 33, no. 2, 1990

***Adrian Kapczyński**, Ph.D. in Computer science, Acting head of division of economical informatics. Areas of interests: security, biometrics, machine learning, computer networks, databases, operating systems, artificial intelligence, project management, computer vision*

***Paweł Kasprowski**, Ph.D. in Computer science, assistant professor in Institute of Informatics. Areas of interests: databases, data mining, machine learning, artificial intelligence, biometrics and biometric identification, text mining.*

***Piotr Kuźniacki**, Ms.C. in Computer science, Areas of interests: security, biometrics, databases, operating systems, programming*