Annals of DAAAM for 2011 & Proceedings of the 22nd International DAAAM Symposium, Volume 22, No. 1, ISSN 1726-9679
ISBN 978-3-901509-83-4, Editor B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2011
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2011

AUTHENTICATION METHOD BASED ON HOLOGRAPHIC SIGNATURE RECOGNITION SYSTEM USING PHYSICAL MODELLING OF A PEN

MIHAILESCU, M[arius] I[ulian]; DIACONESCU, S[tefan] S[telian] & RUSU, S[orin] M[ircea]

Abstract: *Our article discusses a Biometric Recognition System (BRS) that represents a valid solution for security problems regarding the accessibility through internet, even if it isn`t providing an easy and clear environment for users and operators with a medium level of competence. The solution we provide will solve this gap by giving the possibility for users to authenticate in the system through an interface or a simple sheet paper by physical modeling of a hardware pen which emulates the handwritten signature, instead of using the conventional routines for access to the authentication system. In addition, the interface takes in consideration the fail to enroll, as the quality of the signature obtained is calculated during the acquisition time.*
Key words: *biometric, handwritten, holographic signature*

1. INTRODUCTION

This article`s aim is to develop and introduce a new notion and physical device for avoiding unauthorized access to a system. The method represents the hardware proposal of the hardware pen used as kinetic pattern's digital conversion for electronic format of the handwritten signature.

The following system includes an authentication procedure based on handwritten signature, with the purpose to raise the security level for on-line authentication and reduce time allocated for implementing and developing the authentication system by the developers of these types of solutions, by offering this unique service, unbreakable and easy to integrate.

In the theory of holographic algorithms, proposed by Leslie Vailant, the signature plays an important role. The signature theory is substantially developed using holographic algorithms, *d-realizability* and *d-admissibility*.

In this article, we have to take in consideration the fact that the concept of efficient reductions represents one of the most fundamental notion on which the theory of computational complexity is build. [2008b]

Let's imagine the following scenario from Figure 1: you have a paper and a smart pen that is connected to the computer. The person wants to authenticate to the application by writing on the paper its signature. The article takes in consideration the invention and patent [2006] for a computer-based system developed for the acquisition, analysis and authentication of the handwritten signature. The person executing the handwritten signature performs a set of three-dimensional movements with a plane graphical finality. The movements generating kinetic details are received by the special pen (as being performed with bio-kinetic template), and is collected by the MEMS (micro-electro-mechanical-systems) type acceleration sensors in the pen. The systems that we develop continue to analyze the generated information (the signals) and determine the dynamic-biometrical characteristics, based on the biometrical dimension of the information. After this, the characteristics are putted into data vectors and invariants which are stored in the database. The system performs the necessary comparisons between the spatial kinetics of the specimens and the kinetics of the inputs and obtains types of distance answers. If we are looking at this from the point of view of statistical terms, the results are related to the entire subject database, by interpreting and sampling methods.

2. THE PHYSICAL STRUCTUE OF THE AUTHENTICATION SYSTEM

The process of handwritten input nowadays has two points of origin and three targets. Two types for data acquisition are identified: *off-line* and *on-line.* The *off-line* method is characterized by two-dimensional images or pictures of text which are received as input, and in the *on-line* method, the input data are available as a set of signals, representing the movements of the pen.

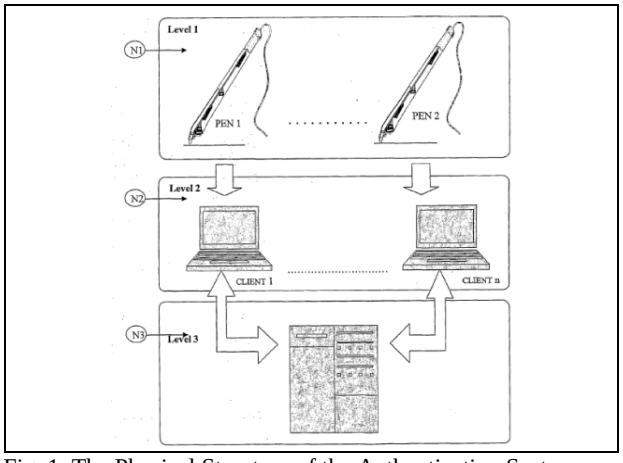

Fig. 1. The Physical Structure of the Authentication System

The system proposed by us is represented on three architectural levels, accomplishing the following:

Level 1 N1: Corresponds to subsystem 1 – S1 consists of two indissoluble entities: the writing device and the kinetic computer-based assembly.

Subsystem 1 – S1. Functions:

1. The pen has dimension and functions assimilative to an ordinary pen, plus the necessary elements and functions to capture, digitize the bio-kinetic patterns and the context information and, then, send them to the second level. The pen shape is given in figure 2.
2. The kinetic computer-based assembly, placed in the pen, has the following functions: acquisition, digital conversion in electronic format of the kinetic pattern and the context information, encoding it in a specific format and

transmitting it to the second level – N2. Of course, here NPL has an important role.

Level 2 (N2): „Client Application" is materialized in subsystem 2 – **S2** and subsystem 3 – **S3** integrated in a personal computer. By its nature, the computer allocates in a sequential or parallel manner the hardware resources to the methods and algorithms implemented in Level 2, thus forming subsystem 2 and subsystem 3 that have the following functions:

Level 3 (N3) is physically materialized by a multiprocessing computer, that allocates in sequential or parallel manner the hardware resources to the methods and algorithms implemented in level 3, thus forming subsystem 4 – S4 and subsystem 5 – S5 which have the following functions:

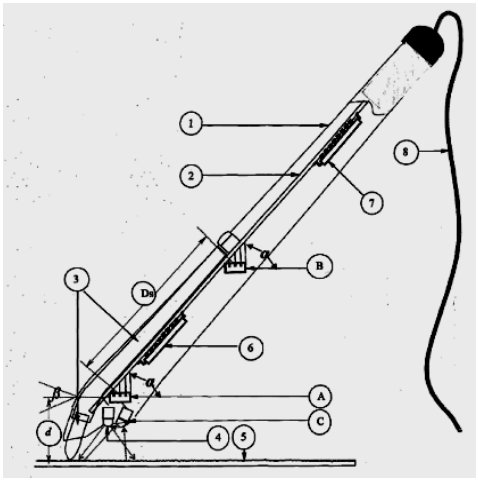

Fig. 2. Subsystem 1 topology-writing and digital conversion of kinetic patterns in electronic format (pen)

The components of the pen are:

1. PCB – printed circuit board
2. MEMS – acceleration sensors Microsystems A, respectively B. Each MEMS microsystem contains two acceleration sensors orthogonally disposed.
3. The IR (Infra-Red) light transmitter 4 sends out a beam with length wave of approximately 800 nn. The beam illuminates in IR the writing paper. The IR light receiver C captures by reflection from paper 5 a quantity of IR light flux proportional to the paper distance and, by means of the analogical comparison instrument from the microcontroller 6. [2010]
4. Microcontroller 6 is used for the acquisition of the information sent by the sensors. The information contained in the bio kinetic pattern is captured, digitized and transferred under the control of a typical program (firmware ASM), that administrates the functioning of the main components integrated in the microcontroller.
5. Integrated micro system 7 for converting and transmitting the acquired data to level 2, in USB format and protocol.
6. USB connection cable 8 for connecting level 1 to level 2. A cable connection was chosen for three main reasons: avoiding unauthorized scanning of the information transmitted to Level 2.

For more information about technical and physical aspects of the pen, it`s necessary to consult the patent [2006].

3. EXPERIMENTAL RESULTS

In this paper, we`ve used many examples of signatures for multimodal biometric authentication. This rate is about 12.5 percents of all. Adding the two mentioned behavioral biometrics (mouse movements and keystroke dynamics) in this solution reduces the need for authentication through multimodal biometric. Another advantage of the proposed system compared with other existing solutions, is the fact that it doesn`t need high bandiwth.

	Attendance rate with a threshold of 2%	Attendance rate with a threshold of 5%	Actual attendance rate
Person 1	98%	98%	100%
Person 2	93%	100%	100%
Person 3	97%	98%	100%
Person 4	90%	95%	100%
Person 5	74%	60%	60%
Person 6	75%	80%	89%
Person 7	49%	9%	50%
Person 8	12%	50%	5

Tab. 1. Attendance rate percentage in virtual environments using the proposed solution

4. CONCLUSIONS AND FUTURE WORK

In this paper we have presented a system for acquisition, analysis and authentication of the handwritten signature, bringing in discussion all the elements that form the system`s project. To capture a substantial part of holographic algorithms, we`ve defined the notion of holographic templates and the device used for signing. It is necessary to understand the theory of holographic algorithms (which isn`t the main subject of the article, but it`s necessary to bring in discussion). For more details, it`s also needed to read and understand the Vailant Leslie`s study about *Holographic Algorithms.* It`s not the right moment to make speculations on the last capability of all the holographic algorithms [2010]. The system project proposes to satisfy the necessities described above by including an authentication method based on holographic signature in all authentication on-line services (banking, eLearning, government, etc.) or, in general, in the entire authentication module in which an internet connection is used. As a future developing line, the system will build a SDK, offered to application developers, which will lead to conceiving facilities of the sub-systems with the authentication role.

4. REFERENCES

R. C., & Clarke, R. (2011). Biometrics and Privacy Biometrics. *Biometrics*, 1-14

Agulla, Gonzales, E., Rua, Argones, Alba, Luis, Castro. (2009) .*Multimodal Biometrics-based on Student Attendance Measurement in Learning Managament Systems*. 11th IEEE International Symposium Multimedia

Sonkamble, S., & Sonkamble, B. (2010). Survey of biometric recognition systems and their applications. *Journal of Theoretical and Applied Information Technology*

Yevgeni, D., Rafail, O., Leonid, R., Smith, A. (2008a). *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data*. *SIAM Journal of Computing*, 38(1):97-139

Reilly, M. A., & Andley, U. P. (2010). Quantitative biometric phenotype analysis in mouse lenses. *Molecular Vision*, *16*, 1041-1046. Molecular Vision

Kholmatov, A., Yanikoglu, B. (2008b) *Realization of correlation attack against fuzzy vault scheme*. In *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, volume 6819 of *Proceedings of SPIE*

*** (2006) System and Methods of Acquisition and Authentification of the Handwritten Signature. Pattent Number WO 2006/085783, http://www. wipo.int/patentscope/search/en/WO200608578