

WEARABLE AUTHENTICATION DEVICE WITH BIOMETRICAL INTRUSION PREVENTION SYSTEM

Sérgio Tenreiro de Magalhães

*Universidade do Minho, Dep. de Sistemas de Informação
Campus de Azurém, 4800-058 Guimarães, Portugal*

Henrique M. D. Santos

*Universidade do Minho, Dep. de Sistemas de Informação
Campus de Azurém, 4800-058 Guimarães, Portugal*

Mário de Araújo

*Universidade do Minho, Dep. de Engenharia Têxtil
Campus de Azurém, 4800-058 Guimarães, Portugal*

Raul Figueiro

*Universidade do Minho, Dep. de Engenharia Têxtil
Campus de Azurém, 4800-058 Guimarães, Portugal*

António Carvalho Santos

*Instituto Politécnico de Coimbra, Escola Superior de Tecnologia da Saúde
Apartado 7006, 3040-162 Coimbra, Portugal*

ABSTRACT

The biometric technologies have been widely used for authentication purposes. But the current needs for security creates the challenge of avoiding attacks before they take place. This can be achieved by combining the traditional biometric technologies with algorithms/tools capable of managing the existing knowledge about emotion recognition. This area has been developed essentially to support the implementation of robots, and for lies detection, and a lot of sensors are already defined and/or proposed to support it. However, in order to use them for real-time human emotion recognition applications, those sensors must be made ubiquitous, non-intrusive and wireless. Besides, given the private nature of the information involved, such a system requires a safe environment for secure storing and processing the user information, like biometric patterns, what SmartCards with processing capabilities can provide. The development of a system so complex requires the development of the biometric algorithms adapted for this purposes, the development of emotions recognition multimodal algorithms and the integration of the resulting components (hardware and software) in a non-intrusive and easy way. In this paper we present the adaptation of a keystroke dynamics algorithm for use in intrusion prevention and we propose a biometrical intrusion prevention system, integrated in a wearable way through the development of a multifunctional textile structure that can supply power to the required microelectronics, while insuring comfort in use. The multifunctional textile structure, besides being comfortable, breathable and washable, has also an active role in assuring the well being of the user once it uses PCM – Phase Change Materials – to keep the user from feeling either cold or hot. Finally, as a probe of concept, it is described a possible application in a healthcare unit (where information security is critical).

KEYWORDS

Wearable, Security, Intrusion, Prevention, Authentication.

1. INTRODUCTION – CATCHING, IN THE PRESENT, THE FUTURE IMPOSTOR

The desire to find out if a person is deseeding has been present throughout the history of the mankind and today the polygraph is a widely used apparatus (81 countries are frequent users of the polygraph), mostly in investigations, pre employment screening and honesty maintenance checks [Damme, G., 2001]. Today, we want/need more: we want/need to stop the fraud before it happens. For that we must insure that only legitimate users can access the systems to be protected (authentication issue) and we must ensure that the legitimate users are, at all the times, trustable (intention issue). An employee that has become greedy may still have access credentials but how do we stop him from harming the organization? After all, a user that accesses a system with bad intentions is also an intruder. The first issue, authentication, has in biometric technologies a good solution when it is possible to provide a safe environment for storing and processing the legitimate patterns [Magalhães, S. and Santos, H., 2003]. The second issue requires an architecture that can predict harming actions of a legitimate user, by his/her wish or by coercion. Biometric data captured and analyzed in the polygraph method, can also be used to detect emotions that are typical of a person that is about to act in a way that is punishable. But, this is not enough, especially for real-time applications, and we need to complement the obtained information with other biometrical information that will allow a strong authentication and a deeper (continuous) understanding of the emotional state of the user. With this information we can define a security context level of the of the user and the security administrators can act accordingly, for instance, requiring emergency passwords to sensitive areas (with limited distribution) or recording the actions taken by the user. This process can be done in an automatic way or by trained personal.

According to Maurice Cusson [Cusson, M., 1993], offenders take in consideration the risk of being caught (and the respective consequences) and act accordingly. He proves more: there is an inhibiting influence that fear exercises over the potential offender; to this influence he calls *situational deterrence*. It is this fear that we will try to detect and, once the target systems are probabilistic, we will try, not to determine if he/she is going to do something bad, but to establish a level of security based on the probability of that wrong behavior.

For a system to be able to provide biometrical authentication and intrusion prevention efficiently, it has to be as non intrusive as possible and easy to use. Wearable solutions are in a privileged position to achieve this, once they can be in physical contact with the user in a long-term intimate way [Picard, R. W. and Healey, J., 1997]. In this paper we present an architecture that implements those ideas in a wearable way, by means of a multifunctional textile structure that can supply power to wireless electronics that are able to capture, store and process biometric data.

1.1 The polygraph

The polygraph is traditionally used to detect lies. But, more precisely, the collected information, respiratory information, Galvanic skin response and cardiac information allows to detect physiological evidence of hypothalamic activity characteristic of a sense of threat [Damme, G., 2001], so we can use it for the purpose of detecting the fear associated to *situational deterrence*.

In fact, the collected data can be used as an indicator of several emotions and there have been some experiences in emotion detection that used this kind of biometrical data. Jolieke Mesken [Mesken, J., 2001] presents several studies that establish a relation between autonomic response and emotions; among the conclusions presented we can point out that:

- Experiencing fear and sadness is accompanied by a higher heart rate,
- Heart rate response is higher in fear than in sadness,
- Fear produces a higher skin conductance than happiness.

Several approaches have also been taken to present a system capable of collecting physiological information in a less intrusive way than the traditional intrusive sensors used by the polygraph. Eurico M. Staderini [Staderini, E. M., 2002] presents a system that uses radar technology to capture that information. It is a non-intrusive system but the wavelength used was out of the authorized limits. Picard [Picard, R. W. and Healey, J., 1997] presents a wearable system that can capture biometrical information but it wasn't wireless and it was not integrated in common clothes.

Nevertheless, as stated by Jolieke Mesken [Mesken, J., 2001] “physiological measures alone are not enough to establish whether an emotion has occurred”. So we need to increase the information captured, as presented by Christine Lisetti [Lisetti, C. L. and Nasoz, F., 2002] in the paradigm of the MAUI project – Multimodal Affective User Interfaces for Everyone. In this paradigm a multimodal framework can take as an input both mental and physiological components associated with emotions. But, until now, there haven’t been any implementations of this paradigm and the nearest system achieved was a wireless arm-bracelet with wireless technology associated with a chest strap, to measure heartbeat, which in a less intrusive way could indicate the emotions felt by its user. The solution to implement the MAUI paradigm may reside in the biometric technologies traditionally used for authentication and in multi-functional textiles.

1.2 Biometric technologies for emotion detection

Some biometric technologies traditionally used for authentication/identification of users are also capable of detecting, with some probability, the emotions felt by a user. That is the case, so far, of facial and voice identification. Later we will show how we intend to use keystroke dynamics – a biometric technology used to authenticate/identify a user based on the way he uses the keyboard – for emotions detection when securing an information system.

Facial recognition is a subject as old as computer vision given the practical implications of the knowledge achieved [Pentland, A. and Choudhury, T., 2000.] The process begins with a image being captured, followed by the detection of a face that will be compared with models stored in a database, complemented with skin color analysis and detection of lines [Thian, N., 2001]. The methods based on this technology are limited by the fact that it is based on locating some predetermined points like the eyes, nose and mouth, which limits the range of accepted positions. Many attempts to apply these technologies in order to obtain facial expression recognition technologies have been made but, so far, the best achievements obtained 80 to 98 percent accuracy when recognizing 5 to 7 classes of emotional expressions in groups from 8 to 32 people. Besides, these values were obtained from very particular situations [Picard, R. W. et al, 2001]. An extended review of the facial expression recognition technologies based on artificial intelligence can be found in the work of Christine Lisetti and Diane Schiano [Lisetti, C. and Schiano, D., 2000].

The processes that use voice recognition are based on the fact that the physical characteristics of each person create unique characteristics to his/her voice. Unfortunately, the information relative to voice that we can capture is insufficient to assure recognition in large scale [Jain, A. et al. 2000]. These methods are based on signal processing technologies and the enrolment of the user can be done by the oral introduction in the system of a pass word/phrase or by the reading of a set of characters that, combined, give to the recognition system sufficient information to assure the authentication or the identification of the person [Markowitz, J., 2000]. The potential of these systems is high due to the low cost of the necessary hardware, a microphone, and there are recent efforts that indicate that there are advantages, for emotion detection, in combining audio and video signals [Picard, R. W. et al, 2001]. Since 1964 it is well known, through the work of Charles McQuinnston, that stress makes natural voice tremors disappear and, since then, many security systems use this information to detect lies [Damme, G., 2001].

The combination of facial and voice recognition is promising, but the recognition of emotions is on a stage similar to the one voice recognition was several decades ago, far from a possible use in every-day tasks [Picard, R. W. et al, 2001]. Best results can only be achieved with an evolution on what we know about emotions and/or on biometric algorithms, or by combining these systems with the ones described in 1.1.

The use of biometrical systems that can also be used for authentication/identification brings up another issue: secure storage and processing of the patterns collected. The safer solution is to use of Smart Cards and we will address that issue in the next section.

1.3 Secure storage with Smart Cards

We call SmartCards to a card with the size of a credit card, with an embedded chip, which may or not be based on a microprocessor. Smart Cards have three kinds of memory: Random Access Memory – RAM – nonpersistent; Electric Erasable Programmable Read Only Memory – EEPROM – persistent and changeable after the production of the card; and Read Only Memory – ROM – burned into the card when produced. The storing and processing capacity is a limiting factor but the evolution of this technology will, as far as it is

predictable, grant more and more capabilities. When the card has a microprocessor, the limitations imposed by the SmartCard hardware are solved by programming the critical parts inside the card and the computational heavy parts inside the terminal to which it will be connected – the host – that can be virtually anything as long as it is equipped with a CAD (Card Acceptance Device) [Chen, Z., 2000]. The connection between the card and the CAD can be made by insertion, by contact or using wireless technologies. The later is the only with interest in our context, once comfort is an issue.

Smart Cards equipped with a processor offer a safe environment for storing and processing biometrical patterns and any other critical information. Besides, it is always under the information owner’s responsibility. We will use them in our architecture.

2. THE DEVELOPMENT OF ACTIVE MULTIFUNCTIONAL TEXTILE STRUCTURES FOR SECURITY APPLICATIONS

The system that we present includes the development of a comfortable textile structure with interior electrical energy conductivity to supply the electronic devices permanently attached to it, such as sensors and a contactless SmartCard. The sensors will capture physical biometric information and send it to the workstation that will process it in order to establish a security level of that moment. The SmartCard will store and process critical data such as biometric patterns for authentication purposes.

The basic concept of developing multi-functional textile structures is one of assembling different types of robust high performance material elements (ex. fibers, particles, microcapsules, additives, etc.) in a particular pre-defined way to perform various specific tasks. The use of yarn and fabric engineering design concepts is essential, together with the most advanced yarn and fabric forming and finishing technologies. Starting with single-functional materials A, B, C, D, E... these may be assembled as shown in Figs.1 and 2. There are two fundamental ways of developing these:

- Multi-functionalised structure with an all-over effect or layered structure, as shown in Fig. 1;
- Multi-functionalised structure with a localized effect or patchwork structure, as shown in Fig. 2.

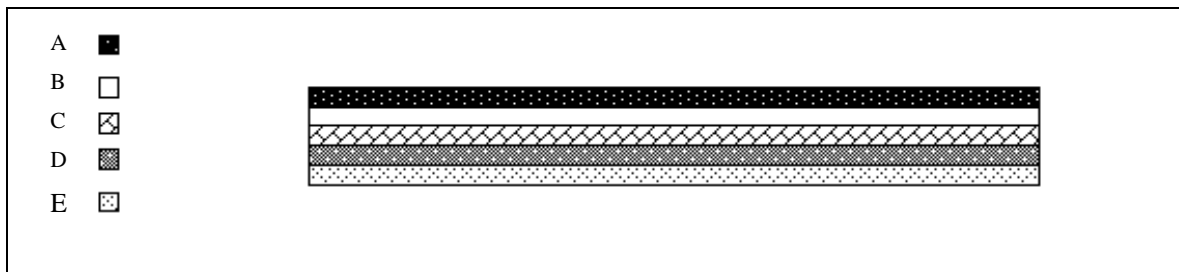


Fig. 1 – Schematic diagram of the cross-section of a multi-functionalized structure with an all-over effect or layered structure

The example given in Fig. 1 may be achieved by knitting (ex. plaiting, sandwich fabrics), weaving (ex. multilayered fabrics), non-woven technologies, coating, laminating and combinations of these.

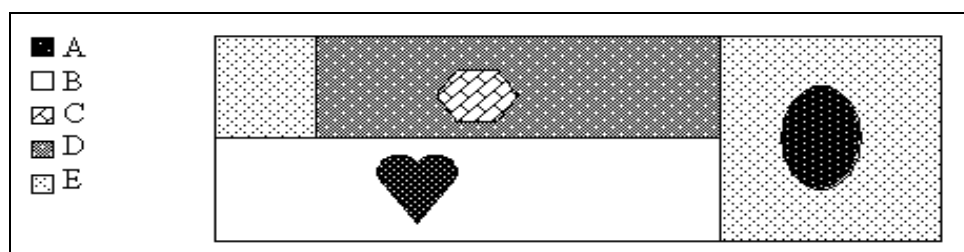


Fig. 2 - Schematic diagram of the technical face of a multi-functionalized structure with a localized effect or patchwork structure

The example shown in Fig. 2 may be possible to achieve by knitting (ex. intarsia, Jacquard), weaving (ex. interchangeable double cloths, Jacquard, multiple weft insertion), embroidery, printing, spraying and combinations of these. Combinations of the various approaches are also possible. Depending on the application, the most suitable materials, structures and technologies to achieve them should be selected.

The structure being developed for use in apparel for security purposes should be comfortable, washable and flexible. In order to achieve thermo-physiological comfort the structure should keep the body at constant temperature and be able to breath in order to transfer body excessive moisture. It should be able to support a variety of wearable electronics for security purposes. The specially designed three-layered structure could be as follows:

1ST LAYER: an open thick structure made of a hydrophobic fiber to be worn close to the skin in order to prevent moisture absorption near to the human body; an elastomeric fiber should be mixed in a small % for snugness;

2nd LAYER (in the interface 1st layer/ 3rd layer): sandwiched between the 1st and 3rd layers runs the network structure of electrically conductive fibers to supply power to the wearable electronics; it should be finished with a micro-encapsulated PCM (phase change material) with a melting point of 28°C in order to create an active thermal barrier between the human body and the atmosphere

3rd LAYER: a highly hydrophilic fiber to be used away from the skin to absorb body moisture with little contact with the human body; it should be porous for breathability and anchored by small channels to the 1st layer to help moisture transfer.

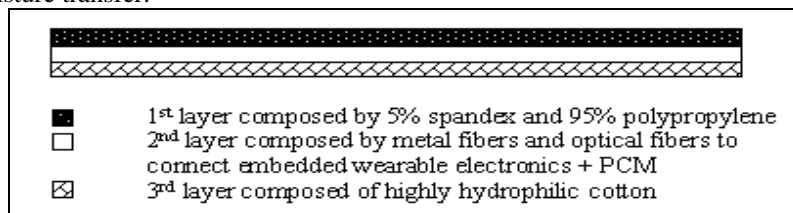


Fig. 3 – Example of cross-section of a possible structure

Other samples will be soon developed using different fibers:

- Conductive fibers based on polyaniline and polypyrrole (2nd layer)
- Fibers with special surface finishing and odd cross-section to induce wicking (3rd layer).

This structure will allow the production of apparel that can host microelectronic devices in a way that can allow the integration of some biometric technologies in a ubiquitous way and, therefore, allowing them to be used as a component of heterogeneous biometrical intrusion prevention systems.

3. KEYSTROKE DYNAMICS AS A BIOMETRICAL INTRUSION PREVENTION TECHNOLOGY

Keystroke dynamics is a behavioral biometric technology that can be used with the collaboration of the user or in stealth mode, and that allows a high precision level, both in authentication and in identification. Furthermore it does not require any special device since it works by analyzing the user keystroke patterns, as he/she types (a password, a passphrase or general text) on a keyboard. Due to the possible integration level, these algorithms can also adjust their parameters to adapt themselves to evolutions of the user typing patterns [Magalhães, S. and Santos, H., 2003]. As in many other problems, there have been two different approaches, machine-learning and deterministic algorithms, to the challenge of finding an algorithm for keystroke dynamics that minimizes the CER – a compromise point where the False Acceptance Rate (FAR) equals the False Rejection Rate (FRR).

Deterministic algorithms are applied to keystroke dynamics since the late 70's. In 1980 [Gaines, R. et al, 1980] Gaines presented a report of his work to study the typing patterns of seven professional typists. The small number of volunteers and the fact that the algorithm is deduced from their data and not tested in other people later, results on a lower confidence on the FAR and FRR values presented. But the method used to establish a pattern was a breakthrough: a study of the time spent to type the same two letters (digraph), when

together in the text. Since then, many algorithms based on Algebra and on Probability and Statistics have been presented.

In [Monrose, F. and Rubin, A. D., 1997] authorized users are clustered according to the number of words typed in a minute and a digital signature vector is calculated for each one of them. Once an anonymous user starts typing, information is collected and a latency time vector is obtained. This vector, U , will be compared with the vectors, R , of the clusters that are in the neighborhood of the one that correspond to his owner's typing speed using the classifier:

$$Score_{Monrose}(R, U) = \sum_{i=1}^N \left(\left[\frac{1}{o_{u_i}} \left[\sum_{j=1}^{o_{u_i}} P \left(\frac{X_{ij}^{(u)} - \mu_{r_i}}{\sigma_{r_i}} \right) \right] \right] * weight_{u_i} \right), \text{ where } \sigma_{r_i} \text{ is}$$

the standard deviation, μ_{r_i} is the average, o_{u_i} is the number of occurrences and $X_{ij}^{(u)}$ is the value of the times in R correspondent to the same digraph of the i value of the U vector; and P is the Normal Distribution.

$$weight_{u_i} \text{ is a function defined by } weight_{u_i} = \begin{cases} 0 & \text{if } u_i \text{ or } r_i \text{ are empty} \\ \frac{o_{u_i}}{\sum_{k=1}^N o_{u_k}} & \text{else case} \end{cases}. \text{ The owner of}$$

the vector from the database that maximizes this classifier is assumed to be the user that is being identified.

We now propose that, in a situation where authentication/identification is already made and if we can assure that there wasn't a user exchange (this is the case once we propose a multimodal system), a first R vector will be recorded some minutes after the authentication occurs. Then, every x minutes (according to the needs for security and capability of the hardware used) a vector U , calculated from the time latencies recorded in those last x minutes, is compared with R , using the $Score_{Monrose}$ classifier. The lower the value achieved by the classifier, the higher will be the probability of the user being altered by a negative emotion, since those are the ones that induce a higher physiological change as presented in [Mesken, J., 2001].

4. THE WEARABLE APPARATUS

The wearable apparatus proposed in this paper it is, from the point of view of the user, a normal piece of clothing. It is made of a comfortable textile structure that can supply power to the wireless electronics that are connected to it on the first layer. This structure is multifunctional and the insertion of the electronics must be made according to the user needs. The proposed electronics include heartbeat, respiration and skin conductivity measuring sensors, a microphone and a wireless SmartCard. The workstation must be equipped with the adequate receptors and with a digital camera.

Information from the user state is permanently captured and, using emotions detection techniques from the several types of technologies involved (as explained before), a security level is determined. If the level is considered dangerous, according to the security police definition, adequate security procedures are fired according to the same security policy.

To enforce privacy, all information that can lead to the user authentication (personal patterns) is stored and processed in a Smart Card and all the data collected is deleted once the user steps away from the workstation. Nevertheless, the last security state should be stored in the card to prevent intentional system reset. Of course, the SmartCard can also be used to store and process acquired biometric information (voice, face and keystroke dynamics patterns) actually used for authentication purposes.

The usability of the apparel is reinforced by the use of PCM in the second layer of the textile structure that, in an active way, will prevent the user from feeling either cold or hot.

5. APPLICATION OF THE WEARABLE APPARATUS IN HEALTHCARE

In a hospital there are two areas of information: the economic/administrative area and the clinical/administrative area. The first contains employee information as well as hospital supplier information. The clinical/administrative information area contains patient records (clinical, diagnostic and therapeutic data), and includes the administrative information concerning healthcare. Not only do patient records serve healthcare, but they also serve a great number of other functions for the healthcare providers [Rindfleisch, T. C., 1997].

For both those information areas, and for most organizations, information security is a central issue. If for the administrative/economic area any data attack may be serious for the operation of the hospital, it can be much more serious if the attack happens in the clinical/administrative information area [Brusil, P. J. and Harley, D., 2002].

The concept of information security has been evolving and it has been present in healthcare for a long time. Doctors have taken the Hippocratic Oath since 4 BC. where the protection of patient privacy is expressed [3]. With the emergence of new other health professions, along with technological evolution patient record confidentiality was broadened beyond the doctor-patient relationship. Now, this is consecrated in most health professions' deontological codes and it should be also enlarged to the information system [Annas, G. J., 2003].

The consequences of confidentiality breaches in clinical/administrative information areas have frequently a high social impact, namely when personal information is published (sexual habits, sexually transmitted diseases, mental diseases, drug habits, etc...) [Cavalli, A. et al, 2004]. But the information confidentiality is not the only issue to keep in mind to what concerns the patient records. The integrity of this type of information is also very important. If information is not integral, it may be cause a wrong treatment decision, with possible serious consequences. Last, but not least important, the information availability, or other way around the unavailability of healthcare information, will almost certainly provoke negative consequences.

Most authors divide healthcare information security into those three dimensions: confidentiality, integrity and availability [Cavalli, A. et al, 2004]. However, others consider that clinical/administrative information has a specific nature and another dimension is required: responsibility/owner [Brusil, P. J. and Harley, D., 2002]. This dimension is the component of security that tries to guarantee, at any moment, the identity of the person who created and/or modified the information.

The proposed apparel can be used to increase the levels of security in healthcare environments by protecting the clinical/administrative information inside the SmartCard. This technology ensures that the information is kept confidential and non-altered (satisfying the first two security properties) and, once the information is in the patient clothes, availability is also ensured. The last healthcare information security dimension, responsibility, can easily be achieved by adding an identifier code to the information registered and, this way, the information creator/modifier's identification is recorded in a safe place. The apparel can also be used to collect biometrical data from the patient in a non-intrusive and permanent way, while actively contributing for the patient comfort. In a hospital environment, this can allow emergency monitoring of the patient biometric data in an emergency situation without the need to transfer the patient for an Intensive Care Unit, or permanent monitoring without the constrains of wire connections in the case, for instance, of pregnant woman. It also allows other comforts to the patient, like body temperature measuring without the need for a stressing wait for the result. Outside the hospital, the apparel can allow permanent monitoring of the patient health situation allowing the patient to contact his doctor if something starts to go wrong or, when adapted to use a GSM/GPRS/UMTS system, automatically alert the emergency response service. Either on a hospital environment or outside of it, the apparel can provide extra comfort to the patient once it has the ability to, actively, prevent the user from feeling cold or hot, given the use of PCM in the textile structure.

6. CONCLUSIONS

In this paper we present architecture for an authentication device with a biometrical intrusion prevention system, that combines biometric measures traditionally used for polygraph devices with emotion recognition tools developed for the construction of human alike robots. The microelectronic wireless devices are incorporated in a new multifunctional textile that is able to provide them with power, while assuring comfort

in use, namely by creating an active barrier to temperature changing. The system provides secure storage and processing of data by means of a SmartCard that is also integrated in the multifunctional textile. The wearability of this system makes it easy to use and the data capture process non-intrusive. We also present a new keystroke dynamics intrusion prevention algorithm, based on an authentication algorithm, used in this wearable system.

The proposed apparatus is designed to prevent harming actions performed by legitimate users of an Information System. Nevertheless, it can also be used for achieving a higher level of security in healthcare environments, as well as a medical instrument, with extra comfort for the patient, both in hospital and out of hospital environment.

REFERENCES

- Annas, G. J., 2003. HIPAA - Regulations - A New Era of Medical-Record Privacy?. *New England Journal of Medicine*. Vol. 348(15), pp. 1486 – 1490.
- Brusil, P. J. and Harley, D., 2002. Medical Records Security. *Computer Security Handbook*, M. E. Kabay, Ed., 4^o ed: John Wiley & Sons, INC.
- Cavalli, A. et al, 2004. Information security concepts and practices: the case of a provinci E.al multi-specialty hospital. *International Journal of Medical Informatics*. Vol. 73, pp. 297-303.
- Chen, Z., 2000. *Java Card Technology for Smart Cards*. Addison Wesley, U.S.A.
- Cusson, M., 1993. Situational Deterrence: Fear During the Criminal Event. R.V. Clarke (ed.). *Crime Prevention Studies*, Criminal Justice Press, Vol. 1. Money. NY.
- Damme, G., 2001. Forensic Criminology and Psycho pathology: Truth Verification Tools with a Special Study of Transfer Pro. *Crime Research In South Africa*. Vol , n.º 1.
- Gaines, R. et al, 1980. Authentication by keystroke timing: Some preliminary results. Rand Report R-256-NSF. Rand Corporation, Santa Monica, CA.
- Jain, A. et al. 2000. Biometric Identification. *Communications of the ACM*, Vol. 43, No. 2.
- Lisetti, C. L. and Nasoz, F., 2002. MAUI: A Multimodal Affective User Interface. *Proceedings of the ACM Multimedia International Conference*. New-York, NY: ACM Press
- Lisetti, C. L. and Schiano, D. J. , 2000. Automatic Facial Expression Interpretation: Where Human-Computer Interaction, Artificial Intelligence, and Cognitive Science Intersect. *Pragmatics and Cognition*.
- Magalhães, P. S. and Santos, H. D., 2003. Biometria e Autenticação. *Actas da 4ª Conferência da Associação Portuguesa de Sistemas de Informação*. Porto. Portugal. CD-ROM edition: ISBN 97 2-9354-42-1.
- Markowitz, J., 2000. Voice Biometrics. *Communications of the ACM*. Vol. 43, No. 9.
- Mesken, J., 2001. Measuring emotions in traffic. *ESF Congress 'Towards Safer Road Traffic in Southern Europe'*. Ankara, Turkey.
- Monrose, F. and Rubin, A. D., 1997. Authentication via Keystroke Dynamics. *Proceedings of the Fourth ACM Conference on Computer and Communication Security*. Zurich, Switzerland.
- Pentland, A. and Choudhury, T., 2000. Face Recognition for Smart Environments. *IEEE computer*.
- Picard, R. W. et al, 2001. Toward Machine Emotional Intelligence: Analysis of Affective Physiological State. *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*. Vol. 23, No. 10.
- Picard, R. W. and Healey, J., 1997. Active wearables. *Personal Technologies* 1: pp 231-240.
- Rindfleisch, T. C., 1997. *Confidentiality, Information Technology, and Health Care*. School of Medicine, Standford University.
- Staderini, E. M., 2002. An UWB radar based stealthy 'lie detector'. *Second Virtual Congress of HRV Scientific Material*.
- Thian, N., 2001. *Biometric Authentication System*, Master thesis, USM, Penang, Malásia.