Study of the Perception on the Biometric Technology by the Portuguese Citizens

Daniela Borges[1], Vítor J. Sá[1], Sérgio Tenreiro de Magalhães[1], and Henrique Santos[2]

[1] FaCiS, Universidade Católica Portuguesa, Campus Camões, 4710-362 Braga, Portugal
[2] DSI, Universidade do Minho, Campus de Azurém, 4800-058 Guimarães, Portugal
minagalhaesborges@hotmail.com,
{vitor.sa,stmagalhaes}@braga.ucp.pt, hsantos@dsi.uminho.pt

Abstract. This article presents the results of a systematic inquiry about the perception of the Portuguese on the biometric technology, which involved 606 citizens. It is presented the principal biometrics and the main concepts on its evaluation. Following a simple method consisting in a survey by questionnaire, the most relevant conclusions are presented.

Keywords: biometrics, reliability, security, cognitive biometrics.

1 Introduction

Because of the needs that have occurred in recent times, in respect to security, biometrics technology is expanding year after year. It consists in the recognition of the individual based on one or more physical or behavioral characteristics and, therefore, some people believe that biometrics is a threat to privacy. Other people do not know the technology at all and others are poorly informed about their capabilities. Due to the lack of consensus, and as a starting point to some potential research in the field, it is useful to have concrete values of these disparities of opinions. With this purpose we conducted a study of acceptance of Portuguese adults to discover the level of familiarity with this type of technology.

In the next section we present the basic concepts and the main biometrics, in section 3 we describe how a biometric system is evaluated, for acceptance or comparison purposes, in section 4 we present the methodology that was followed, including the survey questions, in section 5 we describe the results obtained from the data analysis and, finally, in section 6 some conclusions are drawn.

2 Biometric Technologies

The word biometrics comes from the Greek bios (life) + metron (measure), meaning "measure of life". It is the science that makes the verification of identification of an individual's own characteristics, that is, the automatic recognition of the individual.

In general, access control can be made with the following methods, with its respective advantages and disadvantages:

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 280–287, 2012.

- Card: this is something an individual "has", which can be stolen, forgotten, copied, broken, demagnetized, eventually expires, and has no cogency;
- Password: this is something an individual "knows", which can be copied, must be changed periodically and should not have personal data, and has no cogency that can causes problems in the case of forgetting;
- Biometric technology: this is something an individual "is", which does not lose validity, is not forgotten, is difficult to be copied, is true, is not transferable and is permanent.

The main components of a biometric system are the following: capture (capture of an image or basic information of biometric characteristics), extraction (through a biometric reader, geometric points are extracted, e.g., which will characterize the individual), comparison (matching with stored information) and authentication (decision about the veracity of the recognition).

Biometric technologies are classified into two main categories: those that are related to physical body shape, and those that are related to the behavior of an individual. They can also be classified as collaborative, if they require the user be aware of their existence and consciously participate in the process, or as stealth, if they can be used without the knowledge of the individual that is being identified or authenticated [1].

Recently, a new trend has been developed that merges human perception in a kind of brain-machine interface. This approach has been referred to as cognitive biometrics. Cognitive biometrics is based on specific responses to stimulation of the brain. Currently, cognitive biometrics systems are being developed to utilize the brain's response to stimuli (e.g. the facial expression to the perception of odor). Some systems are based on the functional Transcranial Doppler[1] (fTCD) and functional Transcranial Doppler spectroscopy (fTCDS) to obtain brain responses [2].

In the next subsections, we describe some of the most widely used biometrics.

2.1 Facial Recognition

Facial recognition is a natural method of biometric identification, having as a start point the capture of an image of the face. The identification is not easy because of the constantly changing facial appearance. Causes for different facial expressions are the following: hair style, head position, mustache, angle, lighting conditions, etc. The facial recognition uses distinctive facial features, including contours of the cheeks, sides of mouth and location of the nose and eyes.

2.2 Hand Geometry

Hand geometry is the measurement of the shape of the hand of an individual, which include length, width, thickness, curvature and surface of the hand and fingers. In this method the hand may be well positioned, i.e., the hand must always remain in the same position on the reader device, otherwise the measurements may differ. It is one

[1] Test that measures the velocity of blood flow through the brain's blood vessels.

of the oldest methods that exist, but it is not very precise. It is a fast way of identification and has low cost.

2.3 Fingerprint

The fingerprint is a method that yields great accuracy at low cost, and it is simple and widely used. Fingerprints are unique for each finger of one individual. This method consists in capturing the formation of grooves in the skin of the fingers and palms of an individual. For recognition there are basically three types of technology: optical - to read the fingerprint it is needed a light source; capacitive – consists in the measurement of the temperature that comes from printing and; ultra-sonic – the fingerprints are obtained by using sound signals.

2.4 Iris Recognition

This method is based on reading the colored ring that surrounds the pupil of the eye. Modern systems can be used even in the presence of eyeglasses and contact lenses, and this technology is not intrusive. An important characteristic is that the iris does not change with the person age.

2.5 Retinal Recognition

The reading of the retina is the analysis of blood vessel formation in the back of the eye. It is used a light source to measure the patterns of retinal blood vessels. This method is complex and costly.

2.6 Voice Recognition

The voice recognition works through the spelling of a phrase that acts as a password. The features in voice recognition are based on shape and size of vocal cords, mouth, lips and nasal cavity. This method is associated with the behavioral biometrics, is sensitive because of the person's emotional state and the environment noise, and has a low cost.

2.7 Keystroke Dynamics

This technique is based on the person's behavior when typing text into a keyboard, or the measurement of typing speed. There are several ways to measure the dynamics of typing: the time interval between successive keystrokes; the time a key is pressed; the frequency of typing wrong keys and; the habit of using different keys on the keyboard. This technique has a low cost, due to not require special equipment.

2.8 Signature

The signature is a type of identification that is based on comparing the signature written by an individual with the signature stored in the database, but especially in the dynamics when an individual is signing relatively to its writing speed, direction, movement pressure, rhythm, among others. It's used in banks, although no one signs it the same way, allowing a margin for errors.

3 Evaluation of Biometric Systems

The evaluation of a biometric system suitable for a certain type of application is a complex method that involves different factors. In general the parameters are extracted from the application requirements, being essential to choose the most suitable technology [3]. The assessment can be made between various parameters such as degree of reliability, cost of implementation, level of comfort and acceptance.

The degree of reliability of a biometric system is made by comparing two values: the FRR (False Rejection Rate) and FAR (False Acceptance Rate). These variables are dependent but cannot be both minimized. When the FRR and FAR rates are equal, a balance point was found, which is known by CER (Crossover Error Rate) or EER (Equal Error Rate). The level of comfort and acceptance are user subjective standards but this parameter is crucial for a biometric system. Overall the system is more acceptable as it is less intrusive.

The cost of implementation is a key factor and covers many different factors, some of which are often neglected [4]:

- Hardware
- Software
- Integration with hardware/software available
- Training of users
- Database maintenance staff
- System maintenance

The choice of the method(s) to be used depends on the risk analysis that must necessarily be made relatively to the information/infrastructure to be protected [1].

4 Methodology

Scientific research is a process of systematic deductions that provide information to solve a problem or answer complex questions. This is a systematic and rigorous method. In social sciences, the inquiry produces systematic and accurate research. With a set of relevant social data, explanations can be provided from hypothesis made in advance [5].

The construction of questionnaires is not a simple task. Spending some time and effort in their structure may be a favorable factor in the "growth" of any researcher.

In this work, the choice for data collection and processing falls on the quantitative analysis, since it is more objective, more reliable and more accurate. The quantitative analysis focuses on the use of instruments that quantitatively describe a phenomenon. It also provides a more objective and accurate analysis of the phenomenon, because it uses more standardized techniques for phenomena measurement [6].

One of those techniques is the survey by questionnaire, which was what we used for data collection. According to Raymond Quicky [6], the survey by questionnaire is advantageous because it has the ability to quantify a variety of data and to proceed to a large analysis of correlations.

A questionnaire is a research tool that aims to gather information based, commonly in the inquisition of a representative group of the population under study. This is still extremely advantageous when a researcher wants to collect information on a specific topic within a relatively short time. The questionnaire can be used directly and indirectly. It is used indirectly when the investigator considers the answers that are provided by the respondent and directly when is the proper respondent who fills it.

In order to study the perception on the biometric technology by the Portuguese citizens a survey was prepared and 606 citizens from the Portuguese mainland answered to it. We started to collect some data on the citizen, like living region, gender, age and occupation, and the questions in the survey were the following:

- Do you know the biometric technology?
- From the following types of biometrics indicate which ones do you know?
- Do you think useful to adhere to the biometric technology?
- Have you ever used the biometric technology?
- Do you consider the biometric technology a high-security technology?
- Do you know what cognitive biometrics are?
- If you answered “Yes” to the above question please indicate which ones do you known.

5 Results Obtained

The population in study is represented by 606 respondents. They were mostly females, about 329, while only 277 were male, as Fig. 1 shows. In Fig. 2 we note that the major part of respondents, 215, is from the Southern Region, that 212 represent the Central Region, and 177 correspond to the Northern Region.

As a starting point for any future research on biometric technologies, the conclusion extracted from the next data is relevant, because it demonstrates that most

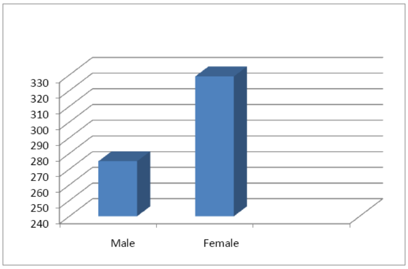

Fig. 1. Number of respondents by gender

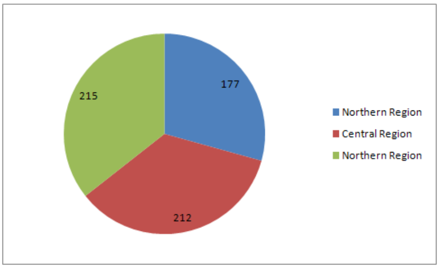

Fig. 2. Number of respondents by region

of the people, 362, don’t know what this kind of technology is about. Only 241 respondents are aware of this (Fig. 3).

The analysis of the types of biometrics that respondents know suggests that fingerprint (215), signature (209), voice recognition (143) and facial recognition (119) are the best known. Likewise, only 97 respondents know the hand geometry, 81 respondents know the retinal recognition and 61 of the respondents know the iris recognition. Finally, 35 respondents know the stroke dynamics, which represents the smallest proportion of individuals (Fig. 4).

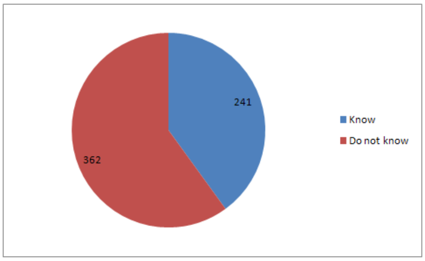

Fig. 3. Who knows biometric technology

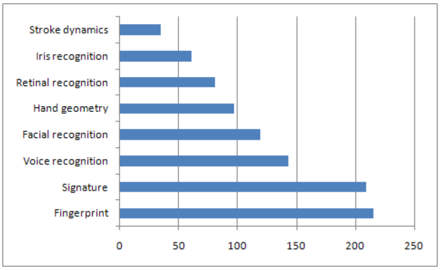

Fig. 4. Types of known biometrics

From the analysis of Fig. 5, below, we can see that 220 of the inquired individuals find it advantageous to adhere to the biometric technology, 38 individuals do not find advantageous to adhere to this technology, and the majority, about 368, chose not to answer this question, which is nevertheless a curious fact.

About the real experience with this kind of technology, most of the respondents already had some contact with biometric recognition. 142 have already used, against 122 that have never used it (Fig. 6).

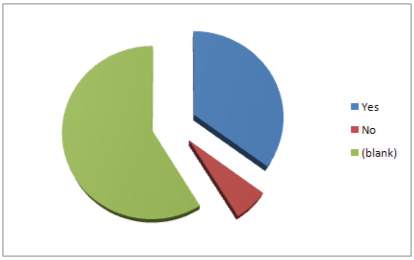

Fig. 5. Respondents that find it advantageous

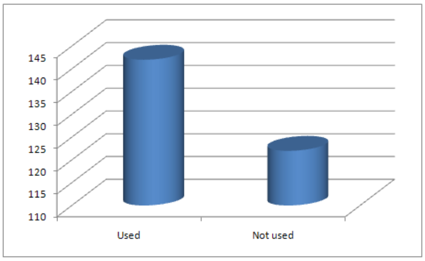

Fig. 6. Respondents who already used

Regarding the level of security deposited by the Portuguese people in the biometric technologies, as shown in figure 7, 64% of the responses consider that they are high security technology, while 36% consider they are not (Fig. 7).

Finally, not less important because it is currently a hot topic in this field, the questionnaire has a question about cognitive biometrics. Without surprise the great majority of the Portuguese people refer that they don´t know what it is, about 246 responses, while only 19 respondents know what this specific group of biometrics is. Fig. 8 shows the correspondent graphic.

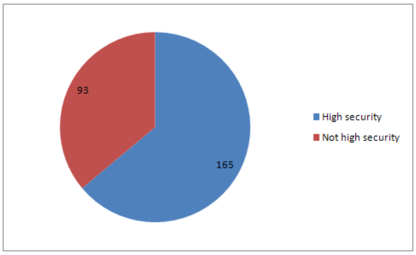

Fig. 7. Biometrics as high security

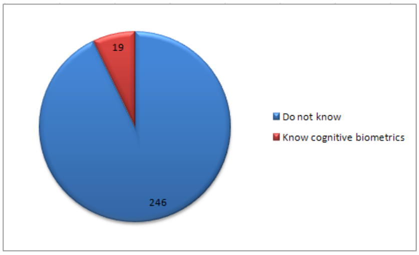

Fig. 8. Who knows cognitive biometrics

6 Conclusion

Throughout this paper, taking into account the amount of collected data, we conclude that respondents, which can represent the Portuguese citizens, did not know the biometric technology in a representative percentage, despite being in a modern country with regard to technological advances. Even being aware of these advances, there are still people (although a small proportion) that do not consider the biometric technology for high security. These can be to the fact that they only had contact with biometrics working on common use devices, like fingerprint or signature, the most well known as shown in Fig. 4. Talking about more specific and new ones, like the cognitive biometrics, the scenario is extreme with a knowledge rate of only 7%.

Other studies of acceptance shows that even in situations where the benefit of such technologies is known, it has no effect on the decision to adopt a biometric technology, because environmental and other organizational characteristics have a major impact in technology adoption [7]. The key consideration in biometric technology adoption is the user acceptance. Alhussain and Drew, 2009, conducted a study that indicated the significant digital and cultural gap between the technological awareness of employees and the preferred authentication solutions promoted by management. It is recommended that an awareness and orientation process about biometrics should take place before the technology is introduced into an organization [8].

We can conclude that something must be done not only in the development and refinement of new security technologies, but also in making people aware of the resulting benefit, and even the real necessity, in many situations.

References

1. Magalhães, P.S., Santos, H.D.: Biometria e autenticação. In: Conferência da Associação Portuguesa de Sistemas de Informação, Porto (2003)
2. Bishop, C., Powell, S., Rutt, D., Browse, N.: Transcranial Doppler measurement of middle cerebral artery blood flow velocity: a validation study. Stroke 17(5), 913–915 (1986)

3. Pinheiro, J.M.: Biometria nos Sistemas Computacionais: Você é a Senha. Ciência Moderna (2008)
4. Liu, S., Silverman, M.: A practical guide to biometric security technology. IT Professional 3(1), 27–32 (2001)
5. Birou, A.: Dicionário das ciências sociais. Dom Quixote, Lisboa (1982)
6. Quicky, R., Campenhoudt, L.: Manual de Investigação em Ciências Sociais. Gradiva, Lisboa (1998)
7. Uzoka, F.-M.E., Ndzinge, T.: Empirical analysis of biometric technology adoption and acceptance in Botswana. Journal of Systems and Software 82(9), 1550–1564 (2009)
8. Alhussain, T., Drew, S.: Towards User Acceptance of Biometric Technology in E-Government: A Survey Study in the Kingdom of Saudi Arabia. In: Godart, C., Gronau, N., Sharma, S., Canals, G. (eds.) I3E 2009. IFIP AICT, vol. 305, pp. 26–38. Springer, Heidelberg (2009)