Enrollment Time as a Requirement for Biometric Fingerprint Recognition

Vítor J. Sá*, Sérgio T. Magalhães
Faculty of Social Sciences
Portuguese Catholic University, Braga, Portugal
E-mail: vitor.sa@braga.ucp.pt
E-mail: stmagalhaes@braga.ucp.pt
*Corresponding author

Henrique D. Santos
Department of Information Systems
University of Minho, Guimarães, Portugal
E-mail: hsantos@dsi.uminho.pt

Abstract. The performance of a biometric system depends on the accuracy, the processing speed, the template size, and the time necessary for enrollment. This last factor is not much addressed in literature. In this work we collected information about the users' availability for enrollment in respect to fingerprint biometrics. Were involved in trials 22 people randomly chosen. The results are presented globally, by sex, by age group and by previous experience in the use of the technology.

Keywords: security, biometrics, enrollment, fingerprint, availability

Biographical notes: Vítor J. Sá holds a five-year "licentiate" degree in Systems and Informatics Engineering and a Masters in Computer Science, both from the University of Minho. He was a Lecturer at the University of Minho and at the Polytechnic Institute of Viana do Castelo, Portugal. He lived for four years in Germany as a Guest Researcher at the Institute for Computer Graphics (Fraunhofer IGD) in Darmstadt, linked to the Technical University of Darmstadt. He has provided consultancy and training to several companies, through the PMO Projects Group. Currently he is a Lecturer at the Portuguese Catholic University. Vítor J. Sá is a Chartered Member of the Portuguese Association of Engineering and has participated and published in several international scientific events, having also published several book chapters. He completed his Ph.D. work in Biometric Authentication.

Sérgio T. Magalhães is an Assistant Professor at the Portuguese Catholic University, Portugal, lecturing Computing Systems and Computer Technology. In the last few years he has developed research in Information Services (especially in information retrieval) and Information Security, more especially in what concerns to behavioural and/or stealth biometric technologies. He is the author of several papers published in international journals and in

international conference proceedings. He is a Member of the Programme Committee of several workshops and conferences in his areas of knowledge. He is the Coordinator of the Scientific Committee of the Master in Safety, Security, Crime and Society from the Portuguese Catholic University.

Henrique D. Santos received his first degree in Electric and Electronic Engineering, by the University of Coimbra, Portugal, in 1984. In 1996 he got his PhD in Computer Engineering, at the University of Minho, Portugal. Currently he is an Associate Professor at the Information Systems Department, University of Minho, being responsible for several graduate and postgraduate courses, as well as the supervision of several dissertations, mainly in the Information Security and Computer Architecture areas. He is also the president of a national Technical Committee (CT 136) related with the information system security standards. During the second semester of 1990, under an ERASMUS program, he was teaching at the University of Bristol, United Kingdom, where he was recognized as University Academic staff.

1 Introduction

In this paper we try to understand to what extent people have patience for the process of enrollment, and argue that this is also one of the requirements of biometric systems, instantiated in this case for fingerprint.

In practical implementation of biometric techniques, it is necessary to take into account the following parameters: performance - a system needs to act quickly and accurately; acceptability - people should accept the system easily; evasion - should not be easy to circumvent the system through fraudulent techniques (Singla & Sharma, 2010). Associated with the second of these parameters, methods for biometrics can also be classified as invasive or non-invasive, according to the level of nuisance that each system triggers in the user.

For the performance of a biometric system several factors contribute to it. Normally the main concern centers on the error rate associated with authentication, leaving part, for example, the time that is required for the enrollment process.

In the next section we present basic concepts of biometric technology, in particular of fingerprint, section 3 is dedicated to motivation and the methodology that was followed, in section 4 we describe the results obtained from the data analysis and, finally, in section 5 some conclusions are drawn.

2 Biometric Technology

Biometrics is the science of measuring individual's own characteristics, making it possible the automatic recognition of people. In the context of information systems the control of who can access certain system can be made with the following methods, with its respective advantages and disadvantages: card - something an individual “has”, which can be stolen, forgotten, copied, broken, demagnetized, eventually

expires, and has no cogency; password - 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 or; biometrics - something an individual “is” or “does”, 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).

The fingerprint is one of the most common biometrics, lying nowadays in many devices of widespread use. Caused by amniotic fluid when the person is still in an embryonic state consists in the texture left forever in the hollow of the hand (Jain, Flynn, & Ross, 2008). In the current state of technology it is possible to distinguish the fingerprint even from identical twins (Jain, Prabhakar, & Pankanti, 2002).

The procedure involves the capture of the image representative of the fingerprint, followed by a segmentation and cut to obtain the image with the largest number of feature points, known as minutiae, which segment is then binarized to be of sufficient quality in order to perform the image analysis for the detection of various patterns (Leon, Sanchez, Aguilar, Toscano, Perez, & Nakano, 2008).

The main problem that arises with this technology is to ensure that the given fingerprint is not a synthetic copy of the original, since it is easy to create a copy even without the consent of its owner (van der Putte, Keuning, & Origin, 2000). To circumvent this problem some readers have sensors to measure temperature, conductivity, blood pressure and/or evaluate patterns that exists in the layer below the epidermis, though with an increase in price (Magalhães, 2008).

The Department of Commerce in the USA held a Vendor Test designated FVC (Fingerprint Verification Competition). This is a test group organized since 2000 by several institutions: the University of Bologna, San Jose State University and Michigan State University. This test has evolved considerably, both in computational demand and the number of algorithms to tender - in 2000 were tested 11 algorithms and in 2002 were tested 31 algorithms, with academic, industrial and anonymous participations. The results show the existence of algorithms with accuracy levels characteristic of a technology with some maturity, but also the existence of embryonic commercial algorithms (Maltoni, Maio & Jain, 2009).

The performance of biometric systems is normally associated to its accuracy, which is determined by the rate of false matches and the rate of false nonmatches (Magalhães & Santos, 2003). The first, known as FAR (False Acceptation Rate or Type II Error), measures the probability of the system to accept an unauthorized person, so the lower the probability the more reliable the system. The second, known as FRR (False Rejection Rate or Type I Error), measures the probability of the system to not recognize an authorized person, so the lower the rate the more the system will be sure of recognizing an individual. As the false acceptances decrease as the level of demand increases and false rejections increase with increase of the same system requirement, there is a balance known as CER (Crossover Error Rate) or EER (Equal

Error Rate), which value is used to classify a biometric system regarding its level of accuracy.

3 Motivation and Methodology

In addition to accuracy to measure the performance of a biometric system, it should also be considered the following factors: the speed, which refers to how quickly a characteristic can be captured, processed into a template, and verified/identified; the size of the templates, which is the amount of bytes required to store a template; and the time necessary to the enrollment. This last factor is not much addressed in literature, so there was the reason for the study presented in this article.

During the enrollment phase, as in the recognition phase, the biometric system measures a characteristic of an individual. First it creates a digital representation of the characteristic that it wants to capture, then the digital representation is processed to create a template (a compact version of the original representation where certain features have been measured) and, finally, the template is stored internally or on an external device such as a Smart card. For this study we developed a simulator in Android environment that supposedly did these procedures.

Thus, to assess the "enrollment availability" by the user it was created an application that simulates the process of fingerprint authentication. In this tool, the process appeared to fail when the user give up trying to enter his data (for example, removing the finger from the sensor) requesting the user to begin again the process (Fig. 1). It were recorded the number of attempts and the corresponding times. Each experiment began with a presentation, by a researcher, of the tool to the user; took place in a closed space and without the presence of any other person (even the investigator left, giving indication that would be available outside to any support); was filmed (with written consent asked to the user) with the argument that it was a scientific research, supposedly with real authentication, which would have to be documented; and terminated when the user requested the support of the investigator that, at that time, explained the true objectives of the experiment.

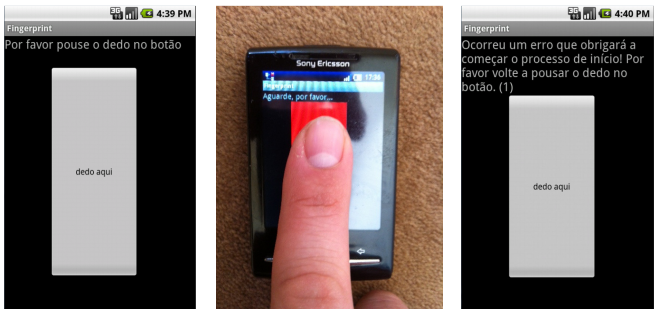

Fig. 1. Simulator interface (before, during and after utilization)

The study has allowed us to collect information about the users' availability for enrollment in respect of fingerprint biometrics. Were involved in trials 22 people

randomly chosen and mostly by academics because we assume by hypothesis that patience is distributed by people without influence of socioeconomic factors. Thus, any sample is representative for this purpose. However, for different sizes we will have different associated confidence intervals and, therefore, different error margins.

4 Results Obtained

We present in the following tables the synthesis of the obtained results globally, by sex, by age group and by previous experience, or not, in the use of fingerprint biometric technology (Tab. 1 and 2). The age division was made according to the Rule of Sturges (Eq. 1), yielding 5 classes for 22 participants.

$$k = 1 + 3{,}3 \log n$$

Eq. 1. Rule of Sturges

For the analysis of Tab. 1 we see that there is an average availability exceeding 10 attempts, and a high standard deviation in both the number of attempts as the average of the average times, which shows large differences between the behaviors of users. However, analyzing the data it appears that, in general, users with less attempts are the ones who spend more time in each trial. Thus, there is a generalized positive predisposition for enrollment that is expressed in some by the predisposition to try for many times and in others to try over a long time, which reveals the existence of two psychological profiles of users as regards this biometric recognition phase.

We chose to present the data by age group despite the low representativeness of the data of each class, as the number of cases studied is relatively small (Tab. 2). However, we understand that the information have any relevance now pointing indicators for future work. These data when divided into age classes can only be regarded as preliminary raise the possibility of being the youngest and the oldest the least available.

Still in relation to the last two columns of Tab. 1 it is apparent that the prior use of the technology of fingerprint authentication does not decrease, on average, the number of attempts that the user is available to accomplish, perhaps because the registration in a fingerprint system always involves repetitions of the capture process.

The results obtained were reassessed limiting our study to the first 12 trials (when they exist) of the users. In none of the studied parameters were found differences of more than one second, it is concluded that users who have tried more than 12 times did not significantly change their behavior over time.

		All	Masculine	Feminine	Already used	Never used
Number of attempts	Mean	12	13	11	13	11
	Minimum	2	2	2	3	2
	Maximum	48	48	38	48	38
	Standard deviation	12.62	15.93	10.93	15.65	11.09
Minimum time		< 1	< 1	< 1	< 1	< 1
Maximum time		407	340	407	407	405
Mean of mean times		48	46	48	45	49
Standard deviation of mean times		58	53	63	56	62

Tab. 1. Results of the assessment of availability for enrollment

		age ≤ 24	25 ≤ age ≤ 30	31 ≤ age ≤ 36	37 ≤ age ≤ 42	43 ≤ age
Number of attempts	Mean	5	17	30	10	4
	Minimum	2	11	5	3	2
	Maximum	8	25	48	32	5
	Standard deviation	2.34	7.09	22.50	9.36	2.12
Minimum time		< 1	< 1	< 1	< 1	14
Maximum time		404	82	228	407	245
Mean of mean times		80	3	19	42	84
Standard deviation of mean times		72	2	26	52	91

Tab. 2. Results by age group of the assessment of availability for enrollment

5 Conclusion

This article contains preliminary results because the sample is not large and did not address other biometrics. For example, there is the idea that people have slightly different behavior in a biometric system by face recognition, because there is a mirror effect that will entertain the user.

The biometrics that was used in this work is the closest to the skin conductivity, in which we have particular interest and we are looking at in terms of acceptance by the population, so the results of this work are very useful in that context.

Acknowledgements

This work was partially funded by FEDER funds through the Operational Program Competitiveness Factors - COMPETE and National Funds through FCT - Foundation for Science and Technology under the Project: FCOMP-01-0124-FEDER-022674.

References

Jain, A.K., Flynn, P.J., & Ross, A.A. (Eds.). (2008). Handbook of biometrics. Springer. New York.

Jain, A.K., Prabhakar, S., & Pankanti, S. (2002). On the similarity of identical twin fingerprints. Pattern Recognition, 35(11), 2653–2663.

Leon, J., Sanchez, G., Aguilar, G., Toscano, K., Perez, H., & Nakano, M. (2008). Fingerprint Recongnition Using Espatial Minutae Information. In: Electronics, Robotics and Automotive Mechanics Conference, 2008. CERMA'08 (pp 381–386).

Magalhães, S.T., & Santos, H.D. (2003). Biometria e autenticação. In: Associação Portuguesa de Sistemas de Informação, Porto.

Magalhães, S.T. (2008). Estudo de viabilidade da utilização de tecnologias biométricas comportamentais na autenticação do cidadão perante os serviços electrónicos do Estado (PhD Thesis). Universidade do Minho, Guimarães.

Maltoni, D., Maio, D., & Jain, A.K. (2009). Handbook of Fingerprint Recognition (2nd ed). London: Springer.

van der Putte, T., Keuning, J., & Origin, A. (2000). Biometrical fingerprint recognition: don't get your fingers burned. In: Smart card research and advanced applications: IFIP TC8/WG8. 8 Fourth Working Conference on Smart Card Research and Advanced Applications, 52, 289-303, Bristol, UK.

Singla, S.K., & Sharma, A. (2010). ECG as Biometric in the Automated World. International Journal of Computer Science & Communication, 1(2), 281–283.