Enrolment Time as a Requirement for Face Recognition Biometric Systems

Vítor Sá[1, 3], Sérgio Magalhães[1, 3] and Henrique Santos[2, 3]
[1]Faculty of Social Sciences, Catholic University of Portugal, Braga, Portugal
[2]Department of Information Systems, University of Minho, Guimarães, Portugal
[3]ALGORITMI Research Center, University of Minho, Braga/Guimarães, Portugal
vitor.sa@braga.ucp.pt
stmagalhaes@braga.ucp.pt
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 enrolment. This last factor is not much addressed in literature. In this work we collected information about the users' availability for enrolment in respect to face recognition biometrics. Were involved in testing 26 randomly chosen people. The results are presented globally, by sex, by age group and by previous experience in the use of the technology. We found that there is a generalized positive predisposition for enrolment that is expressed in some by the predisposition to try for many times and in others to try over a long time, and that it may be the youngest and the oldest the least available.

Keywords: security, biometrics, enrolment, face recognition, availability

1. Introduction

In this paper we try to understand to what extent people have patience for the process of enrolment, and argue that this is also one of the requirements of biometric systems, instantiated in this case for face recognition. This work is based on a similar study conducted for fingerprint recognition (Sá, Magalhães & Santos, 2014).

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 focuses on the error rate associated with authentication, leaving apart, for example, the time that is required for the enrolment process.

In the next section we present basic concepts of biometric technology, in particular of face recognition, section 3 is dedicated to the 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).

Face recognition is one of the most known biometrics (Sá, Borges, Magalhães, & Santos, 2012), lying nowadays in many devices of widespread use. This technology, which reproduces computationally the natural way humans recognize people, has had a major technological development stimulated by the game industry, interested to recognize scammers in their casinos (Liu & Silverman, 2001) and, more recently, by the border control technologies. Proof of this development is the common usage that is currently being given to facial recognition algorithms incorporated both in low photographic devices, as in distributed technologies associated with social networks.

The basic concept associated with this technology is the capture of an image using a camera or video, followed by the recognition of points and/or regions that characterize a human face. These data and the relationships between them are transformed into a multidimensional vector that now constitutes the recognition pattern of the individual. Each of these steps may be performed in various ways.

The image capture phase depends primarily on the quality of the camera. However, the quality is necessarily restricted by the price factor, which determines the adoption of any technology. Associated with the price, but regardless of this, is the kind of camera that will work for normal light or via infrared. This option determines not only the capture conditions but also the processing algorithms. The quality of the camera also condition the number of colours captured, however the use of a large number of colours with implications on the computational and storage requirements may not be desirable.

After the image capture, various techniques can be applied for processing, like the image binarization, the recognition of points/regions by colour neighbourhood, the contours reduction and the subsequent segmentation. Hybrid systems can also be used (Poh & Korczak, 2001).

The above techniques are not specific in biometric recognition, to authenticate/identify the user, but are generic in computer graphics. In order to use the gathered information in the biometric recognition an intermediate stage of image cleaning is required, extracting elements subject to change, such as beard, glasses, haircut, earrings, piercings, etc.

The establishment of patterns is specific to each algorithm in order to recognize the user. Possible approaches rely on conventional statistic techniques, artificial intelligence, or both. These algorithms determine the requirements of pose and lighting (Poh & Korczak, 2001) associated with the image capture and have to take into account the aging factor.

The most important event in this area is the Facial Recognition Vendor Test (FRVT) organized by the Counterdrug Technology Development Program Office of the United States Department of Defence in collaboration with the FBI, the Canadian Passport Office, Australian Customs, the United Kingdom Biometric Work Group, among others. This event was held for the last time in 2012, now in the context of MBE - Multiple Biometrics Evaluation (NIST, 2010), with no results yet available (U.S. Department of Commerce, 2013). Already in 2006 it was achieved a False Rejection Rate of 1% for a False Acceptance Rate of 0.1% (Phillips, Scruggs, O'Toole, Flynn, Bowyer, Schott, & Sharpe, 2010). A curious aspect identified in these studies was a better performance of this technology when applied to males (Phillips, Grother, Micheals, Blackburn, Tabassi, & Bone, 2003).

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 threshold 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 enrolment. This last factor is not much addressed in literature, so there was the reason for the study presented in this article.

During the enrolment 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 "enrolment availability" by the user it was created an application that simulates the authentication process of face recognition. In this tool, the process appeared to fail when the user give up trying to enter his data, 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.

The study has allowed us to collect information about the users' availability for enrolment in respect of face recognition biometrics. Were involved in testing 26 randomly chosen people 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.

Figure 1: Simulator interface (before, during and after utilization)

4. Obtained results

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 face recognition biometric technology (Tab. 1 and 2). The age division was made according to the Sturges's Rule (Eq. 1), yielding 6 classes for 26 participants.

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

Equation 1: Sturges's Rule

For the analysis of Tab. 1 we see that there is an average availability exceeding 20 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 behaviours of users. However, analysing 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 enrolment 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 face recognition authentication does not decrease, on average, the number of attempts that the user is available to accomplish, perhaps because the registration in a face recognition 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, so it is concluded that users who have tried more than 12 times did not significantly change their behaviour over time.

Table 1: Results of the assessment of availability for enrolment

		All	Masculine	Feminine	Already used	Never used
Number of attempts	Mean	21	9	44	13	26
	Minimum	1	1	4	1	1
	Maximum	152	61	152	66	152
	Standard deviation	37.75	14.92	55.70	23.47	42.80
Minimum time		<1	<1	<1	<1	<1
Maximum time		639	639	94	355	639
Mean of mean times		86	128	8	100	62
Standard deviation of mean times		121	133	13	127	93

Table 2: Results by age group of the assessment of availability for enrolment

		a≤23	24≤a≤27	28≤a≤31	32≤a≤35	36≤a≤39	a≥40
Number of attempts	Mean	19	9	9	-	152	23
	Minimum	1	2	3	-	152	2
	Maximum	119	17	21	-	152	61
	Standard deviation	34.87	5.2	10.12	-	-	32.97
Minimum time		<1	<1	<1	-	<1	<1
Maximum time		422	639	297	-	38	572
Mean of mean times		118	30	37	-	3	140
Standard deviation of mean times		146	27	62	-	-	147

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 behaviour 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 others 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. As future work we intend to do similar studies regarding other biometrics.

Acknowledgements

This work has been supported by FCT – Fundação para a Ciência e Tecnologia within the Project Scope: PEst-OE/EEI/UI0319/2014.

References

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

Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. IT Professional, 3(1), 27–32.

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

NIST, (2010). MBE Multiple Biometric Evaluation, NIST, USA.

Sá, V.J., Borges, D., Magalhães, S.T., & Santos, H.D. (2012) "Biometric technologies and their perception by the common citizen", *International Journal of Electronic Security and Digital Forensics*, 4(2), 187-200.

Sá, V.J., Magalhães, S.T. & Santos, H.D. (2014) "Enrolment Time as a Requirement for Biometric Fingerprint Recognition", *International Journal of Electronic Security and Digital Forensics*, 6(1), 18-24.

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

Phillips, P. J., Grother, P., Micheals, R., Blackburn, D. M., Tabassi, E., & Bone, M. (2003). Face recognition vendor test 2002. In: IEEE International Workshop on Analysis and Modelling of Faces and Gestures, AMFG 2003 (p 44).

Phillips, P. J., Scruggs, W. T., O'Toole, A. J., Flynn, P. J., Bowyer, K. W., Schott, C. L., & Sharpe, M. (2010). FRVT 2006 and ICE 2006 Large-Scale Experimental Results. IEEE Transactions on Pattern Analysis and Machine Intelligence, 32(5), 831–846.

Poh, N., & Korczak, J. (2001). Hybrid Biometric Person Authentication Using Face and Voice Features. In: J. Bigun & F. Smeraldi (Eds), Audio- and Video-Based Biometric Person Authentication (Vol 2091, pp 348–353), Springer, Berlin/Heidelberg.