DYNAMIC SIGNATURE RECOGNITION FOR AUTOMATIC STUDENT AUTHENTICATION

Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, Javier Ortega-Garcia

Departamento de Tecnologia Electronica y de las Comunicaciones, EPS, Universidad Autonoma de Madrid (SPAIN)

Abstract

Handwritten signatures are one of the most socially accepted biometric traits. Signatures are commonly used in financial and legal agreements since more than a century. In education, signatures are used for attendance control, either to lectures or exams, but not for (automatic) authentication. With the rapid deployment of dynamic signature recognition, this technology is ready to be used for student authentication. Also, the use of this technology can be extended to different administrative services within the education system, in order to add a higher security level to the traditional procedures of authentication (e.g., visually checking the face and/or signature on the person identity card).

Nowadays, signatures can be easily captured by means of electronic devices (e.g. pen tablets, PDAs, grip pens, smartphones, etc.). For this reason, the popularity of this biometric trait is rapidly increasing in the last few years. Even more, signatures can be made using the finger as the writing tool on smartphones. In this paper, we analyse two scenarios for student authentication using their signatures: i) an office scenario with a high quality pen tablet specifically designed to acquire signatures (i.e., Wacom device), and ii) a mobile scenario where users sign on their smartphones with the finger improving this way the usability. For this experimental study we make use of e-BioSign database, which was captured using various modern pen tablet devices and smartphones. The database contains signatures from 70 users including students and educators, captured in two sessions in different days. The experiments on automatic authentication using dynamic signatures are conducted considering two different types of forgeries, namely: i) random forgeries (the case where an impostor uses his own signature claiming to be another person), and ii) skilled forgeries (where impostors imitate the signature of other persons).

Keywords: Innovation, person authentication, signature recognition, biometrics.

1 INTRODUCTION

User authentication in different services and systems is a critical need in many scenarios nowadays. Biometric recognition systems have many advantages compared to traditional schemes, which are based on what the user knows (passwords, keys, etc.) or what the user has (card, token). In this sense, biometric traits cannot be lost, it is not necessary to memorize them as they are part of ourselves. In fact, we can consider biometric authentication as a mature technology, and systems based on fingerprint, iris or face recognition, are already common in access controls at airports and are stored on our identity cards and passports. However, there are many challenges still to be resolved.

The different biometric traits can be classified according to their nature, in: a) physiological or morphological traits, such as fingerprint and palm print, the iris, face, hand geometry and the ear, or hand vein pattern; b) behavioral traits, arising from any conduct or human behavior, and generated from something that the person produces, such as the voice, signature and handwriting, or the way people walk, among others.

In this paper we focus on the application of biometric recognition for automatic student authentication, in particular making use of handwritten signatures, which are one of the most socially accepted biometric traits. Signatures are commonly used in financial and legal agreements since more than a century. In education, signatures are used for attendance control, either to lectures or exams, but not for (automatic) authentication. With the rapid deployment of dynamic signature recognition [1], this technology is ready to be used for student authentication. Also, the use of this technology can be extended to different administrative services within the education system, in order to add a higher security level to the traditional procedures of authentication (e.g., visually checking the face and/or signature on the person identity card).

The use of dynamic signatures has huge advantages in user authentication processes, as they are perceived as natural in an authentication process, the dynamic process of writing cannot be extrapolated completely from visually displaying how the signature was done, as there is identity information that is not reflected in the graph.

Nowadays, signatures can be easily captured by means of electronic devices (e.g. pen tablets, PDAs, grip pens, smartphones, etc.) [2]. For this reason, the popularity of this biometric trait is rapidly increasing in the last few years. Even more, signatures can be made using the finger as the writing tool on smartphones [3, 4]. These devices represent an attractive target for the deployment of a signature verification system, providing enough processing capabilities and a touch-based interface [8]. However, signature verification on handheld devices is affected by factors not present in other input devices primarily because of a small input area, poor ergonomics or the fact that the user may be in movement. Users must sign on an unfamiliar and usually unstable surface with a small stylus or a finger. As a consequence, the signature generation process may be degraded.

In this paper, we analyze two scenarios for student authentication using their signatures: i) an Office Scenario with a high quality pen tablet specifically designed to acquire signatures (i.e., Wacom device), and ii) a Mobile Scenario where users sign on their smartphones with the finger improving this way the usability. This is a very novel case of study in the field of dynamic signature recognition, as the great majority of research has been conducted using pen tablets or mobile devices but using pen stylus and not the finger [5, 6, 7].

The first case considered is thought to include automatic user authentication in conventional scenarios where user authentication using their signature is common (for example university administrative services). The second case of automatic user authentication in a mobility scenario opens the door to many different applications as the users own the sensor needed for the signature acquisition (smartphone). So in education there are applications for user authentication in MOOCS, attendance control in lectures or exams, use in libraries, etc., also in others sectors such as e-government, healthcare, banking or insurance. Based on the experimental results we comment on the usage convenience of each of them in different applications based on the security level restrictions.

For this experimental study we make use of the e-BioSign database [4], which was captured using various modern pen tablet devices and smartphones. The database contains signatures from 70 users including students and educators, captured in two sessions in different days. The experiments on automatic authentication using dynamic signatures are conducted considering two different types of forgeries, namely: i) random forgeries (the case where an impostor uses his own signature claiming to be another person), and ii) skilled forgeries (where impostors imitate the signature of other persons).

2 USER AUTHENTICATION USING DYNAMIC SIGNATURE

Dynamic signature verification systems generally share a common architecture as the one shown in Figure 1.

1. **Data Acquisition:** For data acquisition we consider in this study two devices, a digitizing tablet (Wacom STU-530) and a smartphone (Samsung Galaxy Note 10.1) to study the system performance in two different applications (office and mobile).
2. **Data Preprocessing:** The preprocessing step consisted in removing the initial and final samples with no pressure, keeping this way only the information between the first and last pen-downs. Also a step consisting on position normalization was performed by aligning the center of mass of each signature to a common coordinate.
3. **Feature Extraction:** There are two main feature extraction approaches in dynamic signature verification: feature-based and function-based systems. In this case we followed a function-based approach, based on a selection of time signals extracted from the X, Y and pressure signals, such as their first and second order derivatives, the velocity, the curvature radius, etc. (see [9] for further details).
4. **Similarity Computation:** This step involves pre-alignment if necessary and a matching process, which returns a matching score. In this case, Dynamic Time Warping (DTW) algorithm is used as the classifier, which allows computing an elastic alignment between time sequences of different length, and obtaining a distance measure.

5. **Score Normalization:** The final step is score normalization, where the matching scores are normalized to a given range. Score normalization is critical when combining scores from multiple classifiers or in multi-biometric systems.

Finally, an input signature will be considered from the claimed user if its matching score exceeds a given threshold.

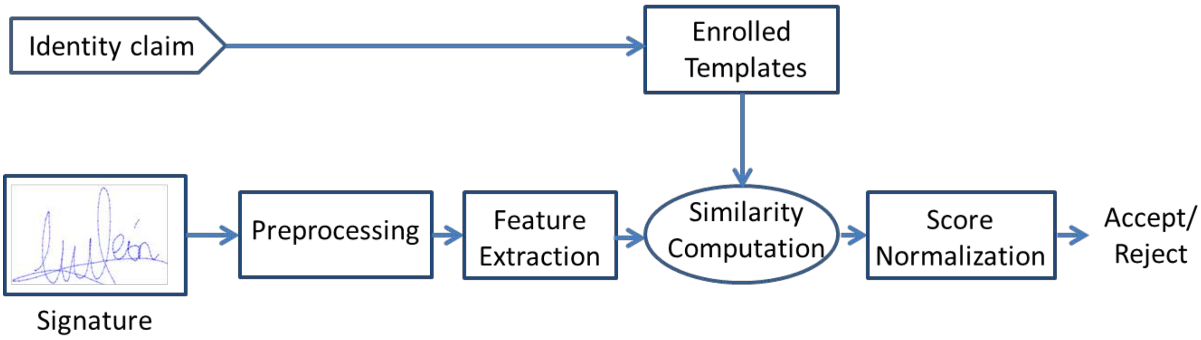


Figure 1. Arquitecture of a dynamic signature verification system.

3 DATABASE AND EXPERIMENTAL PROTOCOL

3.1 Database Description

The experiments carried out in this work are performed using a subset of e-BioSign database [4]. In this case we have used two of the five devices: Wacom STU-530 and Samsung Galaxy Note 10.1 (see Figure 2). The first one (Wacom) is specifically designed for capturing handwritten data and will be used in this study to simulate an office scenario. The second device (Samsung) is a general purpose device not specifically design for capturing dynamic signatures, and will be used in this study in a mobile scenario where users can sign with their fingers.

- **Wacom STU-530**: 5-inch TFT-LCD color display, with VGA resolution of 640 x 480 pixels. It has a sampling rate of 200 Hz, and 1024 pressure levels. This device only allows writing using a pen stylus.
- **Samsung Galaxy Note 10.1**: This is a device with Android OS. It has a 10.1-inch LCD display with a resolution of 1280 x 800 pixels. It has 1024 pressure levels. This device allows to use both a pen stylus or the finger.

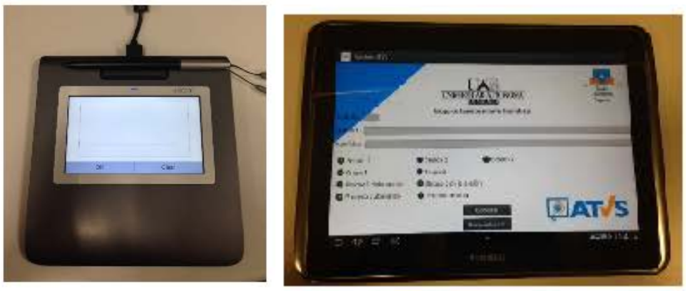
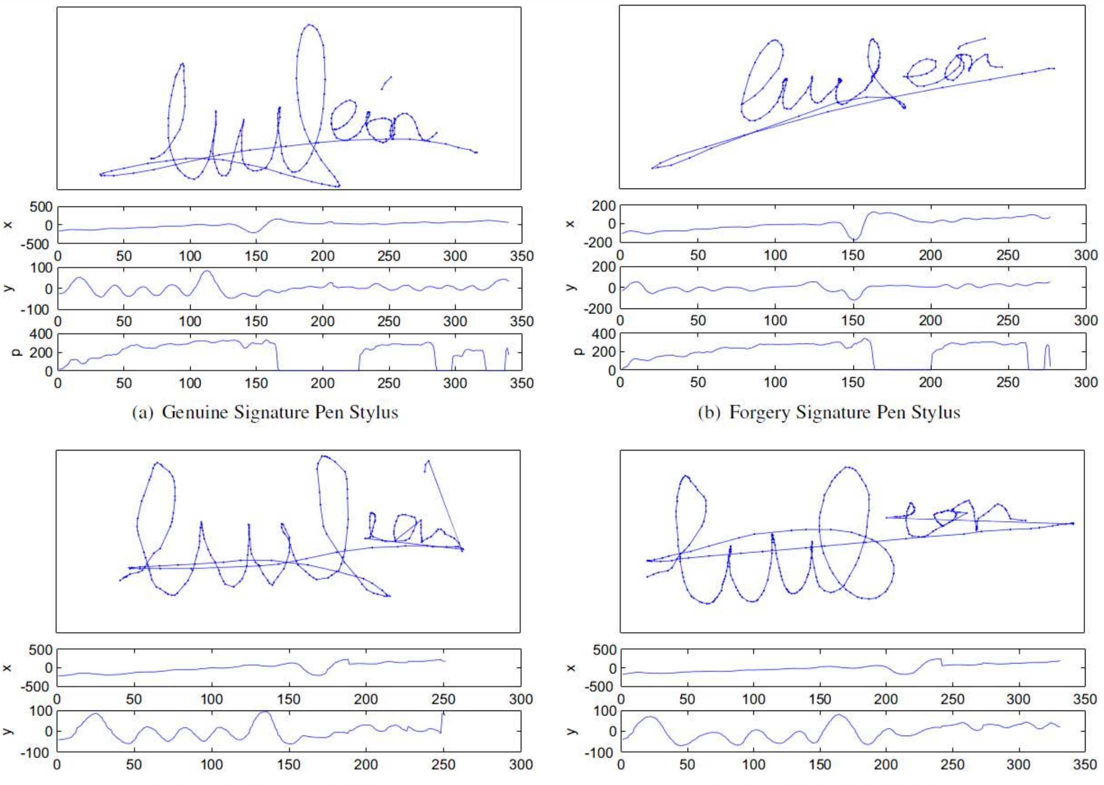


Figure 2. Devices used in this study to acquire dynamic signatures.
Left, Wacom STU-530, and right, Samsung Galaxy Note 10.1.

e-BioSign database was collected in two sessions with a time gap of at least three weeks between them. In each session 4 genuine signatures and 3 skilled forgeries were acquired for each of the 70 users of the database.

The whole capturing process was supervised by an operator who explained all the steps that donors had to follow. Therefore this is a multi-session and multi-device database with samples captured using a pen stylus and the fingertip for signature data. Figure 3 shows examples of the data collected in e-

BioSign for the Samsung Galaxy Note 10.1 device, with genuine and forgeries signatures using the pen stylus and the finger. It is worth noting that data collected using the finger for the Samsung Galaxy Note 10.1 do not contain pressure information as this was not provided by this device, and also there is no information of the trajectory (X and Y coordinates) when having a pen-up. For the case of using the pen stylus with the Wacom device the information of pressure and pen-up trajectories is available and has been used in the evaluation reported in this paper.



(a) Genuine Signature Pen Stylus

(b) Forgery Signature Pen Stylus

(c) Genuine Signature Finger

(d) Forgery Signature Finger

Figure 3. Example of the data collected in e-BioSign database for Samsung Galaxy Note 10.1.

Figure 4 shows the statistics of the population of e-BioSign database. Regarding the age distribution, the majority of the subjects (67.1%) are between 22 and 27 years old (mainly university undergraduate and postgraduate students), as the database was collected in a university environment. Then 11.4% are between 17 and 21 years old, also 11.4% are between 28 and 38 years old and 10% are above 39 years old. Table 1 shows the age distribution and also the gender and handedness distributions. The gender was designed to be as balanced as possible, having 58.6% of males and 41.4% of females. Regarding the handedness distribution, 88.6% of the population is righthanded.

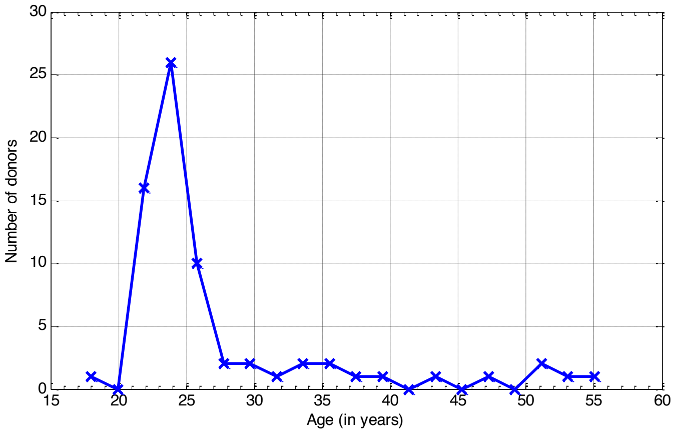


Figure 4. Age distribution of e-BioSign Database.

Table 1. Population statistics of e-BioSign Database.

Age distribution (17-21 / 22-27 / 28-38 / >39)	11.4% / 67.1% /11.4% /10%
Gender distribution (male / female)	58.6% / 41.4%
Handedness distribution (righthanded / lefthanded)	88.6% / 11.4%

3.2 Experimental protocol

The experimental protocol was designed to obtain a baseline performance comparison for the two scenarios of interest for person recognition using dynamic signature, i.e., office scenario (Wacom device with stylus) and mobile scenario (Samsung device with finger). In this evaluation no user model was trained, so the results are based on 1 to 1 signature comparisons. In this way, a leave-one-out approach was used with the eight genuine signatures of each user.

Two types of forgeries are considered in our experiments: “Random forgery” scores (the case where a forger uses his own signature claiming to be another user of the system) are obtained by comparing the user genuine signatures to one signature sample of all the remaining users. “Skilled forgery” scores are computed comparing the genuine signatures with the 6 available skilled forgeries per user.

4 EXPERIMENTAL RESULTS

This section describes the baseline experimental results obtained for the two operational scenarios considered in this paper.

In a verification system there are two types of errors that can be made. If the system accepts an impostor it is a False Acceptance. The rejection of a valid claim is a False Rejection. To evaluate the performance of a verification system, a set of true and impostor trials is processed.

The overall performance of a verification system can be analysing plotting DET (detection error tradeoff) curves (see Figure 5), which is a plot of points with False Acceptance probability on the vertical axis, and the False Rejection probability on the horizontal axis.

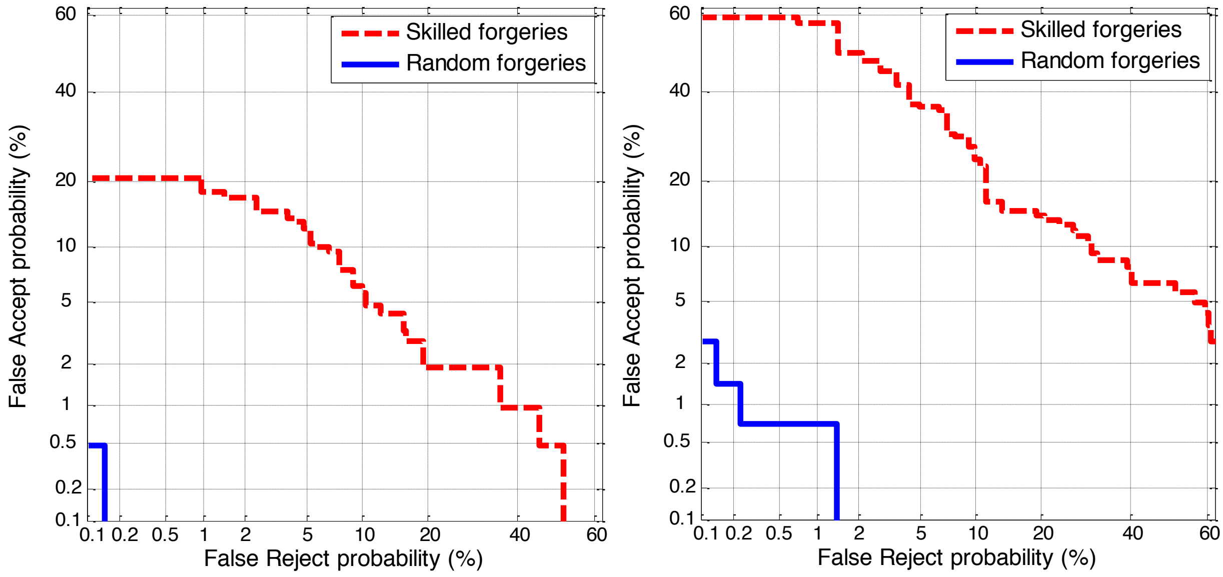
A popular performance measure is to give the equal error rate (EER) which is the operation point where the False Acceptance probability and the False Rejection probability have the same value. The lower the EER, the better the biometric system.

In the experimental work carried out in this paper, signature verification performance is reported in terms of equal error rates (EERs) in Table 2 and DET curves in Figure 5. As can be seen in both Table 2 and Figure 5, in general terms the biometric system performance achieved in the Office Scenario is better compared to the mobile scenario. Equral error rates obtained for the Office Scenario are around half the value with 0.3% EER for random forgeries compared to 0.7% EER obtained in the Mobile Scenario. And 7.6% EER for Office Scenario compared to 14.9% EER for Mobile Scenario in a case of having skilled forgeries.

While this difference in performance is significant, results achieved in the Mobile Scenario are acceptable for skilled forgeries and very good for random forgeries. Reasons for this difference in performance can be a few, such as, the pressure information is not recorded by mobile devices while signing with the finger, also pen-up information is not recorded, and writing with the finger can produce a higher signature intra-person variability compared to signing with a pen stylus.

Table 2. Performance (EER) for the operational scenarios considered.

Scenarios Considered	**Equal Error Rates (%)**	
	Skilled Forgeries	**Random Forgeries**
Office Scenario	**7.6**	**0.3**
Mobile Scenario	**14.9**	**0.7**



a) Office Scenario

b) Mobile Scenario

Figure 5. DET curves results for the two operational scenarios considered in this study, showing for each case both skilled and random forgeries results.

5 CONCLUSIONS

This work analyses two scenarios for student authentication using their signatures: i) an office scenario with a high quality pen tablet specifically designed to acquire signatures (i.e., Wacom device), and ii) a mobile scenario where users sign on their smartphones with the finger improving this way the usability. For this experimental study we have made use of e-BioSign database, which was captured using various modern pen tablet devices and smartphones. The database contains signatures from 70 users including students and educators, captured in two sessions in different days. The experiments on automatic authentication using dynamic signatures are conducted considering two different types of forgeries, namely: i) random forgeries (the case where an impostor uses his own signature claiming to be another person), and ii) skilled forgeries (where impostors imitate the signature of other persons).

Experiments have shown very good recognition performance in office scenarios (0.3% EER for random forgeries and 7.6% EER for skilled forgeries). In mobile scenarios performance is very good against random forgeries detection (0.7% EER), but degrades to 15% EER in cases of skilled forgeries. There is still room for improvements of these results, for example training user models with some signatures (around 5 to 10). This way the intra-person variability can be included in the models producing improvements of performance. Therefore, we strongly support the usage of this technology in a university educational environment for automatic person authentication.

REFERENCES

[1] J. Fierrez and J. Ortega-Garcia, "On-line Signature Verification", A. K. Jain, A. Ross and P.Flynn (Eds.), *Handbook of Biometrics*, Springer, pp. 189-209, 2008.

[2] M. Martinez-Diaz, J. Fierrez, “Signature Databases and Evaluation”, Encyclopedia of Biometrics’ Springer, pp. 1178–1184, 2009.

[3] M. Martinez-Diaz, J. Fierrez and J. Galbally, "The DooDB Graphical Password Database: Data Analysis and Benchmark Results", *IEEE Access*, Vol. 1, pp. 596-605, 2013.

[4] R. Vera-Rodriguez, R. Tolosana, J. Ortega-Garcia and J. Fierrez, "e-BioSign: Stylus- and Finger-Input Multi-Device Database for Dynamic Signature Recognition", in Proc. 3rd International Workshop on Biometrics and Forensics (IWBF), IEEE Press, 2015.

[5] N. Houmani, A. Mayoue, S. Garcia-Salicetti, B. Dorizzi, M. Khalil, M. Moustafa, H. Abbas, D. Muramatsu, B. Yanikoglu, A. Kholmatov, M. Martinez-Diaz, J. Fierrez, J. Ortega-Garcia, J. R. Alcobé, J. Fabregas, M. Faundez-Zanuy, J. Pascual-Gaspar, V. Cardeñoso-Payo and C. Vivaracho-Pascual, "BioSecure signature evaluation campaign (BSEC2009): Evaluating online signature algorithms depending on the quality of signatures", Pattern Recognition, ISSN 0031-3203, Vol. 45, n. 3, pp. 993-1003, March 2012.

[6] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M. Freire, J. Gonzalez-Rodriguez, C.Garcia-Mateo, J.-L.Alba-Castro, E.Gonzalez-Agulla, E.Otero-Muras, S.Garcia-Salicetti, L.Allano, B.Ly-Van, B.Dorizzi, J.Kittler, T.Bourlai, N.Poh, F.Deravi, M.Ng, M.Fairhurst, J.Hennebert, A.Humm, M.Tistarelli, L.Brodo, J.Richiardi, A.Drygajlo, H.Ganster, F.M.Sukno, S.-K.Pavani, A.Frangi, L.Akarun and A.Savran, "The Multi-Scenario Multi-Environment BioSecure Multimodal Database (BMDB)", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 32, n. 6, pp. 1097-1111, June 2010.

[7] S. Garcia-Salicetti, J. Fierrez-Aguilar, F. Alonso-Fernandez, C. Vielhauer, R. Guest, L. Allano, T. D. Trung, T. Scheidat, B. L. Van, J. Dittmann, B. Dorizzi, J. Ortega-Garcia, J. Gonzalez-Rodriguez, M. B. d. Castiglione and M. Fairhurst, "Biosecure reference systems for on-line signature verification: A study of complementarity", Annals of Telecommunications, Special Issue on Multimodal Biometrics, Vol. 62, n. 1-2, pp. 36-61, January-February 2007.

[8] C. Vivaracho-Pascual, J.M. Pascual-Gaspar, “On the use of mobile phones and biometrics for accessing restricted web services”, IEEE Trans. Syst. Man Cybern. C, Appl. Rev., 42, (2), pp. 213–222, 2012.

[9] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia and J. Fierrez, "Preprocessing and Feature Selection for Improved Sensor Interoperability in On-Line Biometric Signature Verification”, IEEE Access, 2015.