Secure Access System Using Signature Verification over Tablet PC

Fernando Alonso-Fernandez, Julian Fierrez-Aguilar,
Javier Ortega-Garcia & Joaquin Gonzalez-Rodriguez
Universidad Autonoma de Madrid

ABSTRACT

Low-cost portable devices capable of capturing signature signals are being increasingly used. Additionally, the social and legal acceptance of the written signature for authentication purposes is opening a range of new applications. We describe a highly versatile and scalable prototype for Web-based secure access using signature verification. The proposed architecture can be easily extended to work with different kinds of sensors and large-scale databases. Several remarks are also given on security and privacy of network-based signature verification.

INTRODUCTION

Personal authentication in our networking society is becoming a crucial issue [1]. In this environment, there is a recent trend in using measures of physiological or behavioral traits for person authentication, which is also referred to as biometric authentication. Biometrics provides more security and convenience than traditional authentication methods which rely in what you know (such as a password) or what you have (such as an ID card) [2]. Within biometrics, signature verification has been an intense field of study due to its social and legal acceptance [3, 4].

In this paper, we present a prototype for Web-based secure access using signature verification. The increasing use of low-cost portable devices capable of capturing signature signals such as Tablet PCs, mobile telephones or PDAs is resulting in a growing demand of signature-based authentication applications. Our prototype uses a Tablet PC for signature acquisition [5] but it can be easily extended to other signature acquisition devices as well.

WEB-BASED SECURE ACCESS USING SIGNATURE VERIFICATION

The global architecture of our prototype is shown in Figure 1. A signature verification server manages the verification process. This server communicates with a web server, which manages the communication with the user terminal using the HTTP protocol through a network. In our prototype, the user terminal is a Tablet PC and both the web server and the signature verification server are installed in a standard PC that communicates with the Tablet PC thorough a LAN.

The proposed architecture is highly versatile. User terminal can be any device capable of capturing on-line signatures, from cheap digitizing tablets to more expensive Tablet PCs [5]. It is also highly scalable, since we can use powerful servers capable of managing several transactions in parallel, not only HTTP-based but using any other secured or unsecured protocols. Table 1 summarizes several applications that can use the proposed architecture.

This architecture can also be adapted to work in other situations such as:

- The signature verification server has low storing capacity. Users can be provided with a smartcard with its statistical model stored in it [6]. This approach saves considerable hard disk space in the central server and avoids the statistical models being stolen by a hacker or accidentally deleted by system administrators. On the contrary, the statistical model has to be transferred through a network and thus they can be intercepted by other users if no encryption or secure connection is used.

- The signature verification server has low processing capacity. The user terminal can then be allowed to perform the verification process, notifying the central server the acceptation/rejection decision. This approach saves considerable processing power in the signature verification server and reduces the amount of data to be transferred. In addition, the user templates are never transmitted, so they cannot be intercepted. On the other hand, we

Refereeing of this work was handled by R.C. McMillan.
Manuscript received December 16, 2005; revised June 16, 2006.
Released for publication September 30, 2006.

Author's Current Address:
F. Alonso-Fernandez, J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, Escuela Politecnica Superior, Universidad Autonoma de Madrid, Ctra. Colmenar km. 15, E-28049 Madrid, Spain.

0885/8985/07/ USA $25.00 © 2007 IEEE

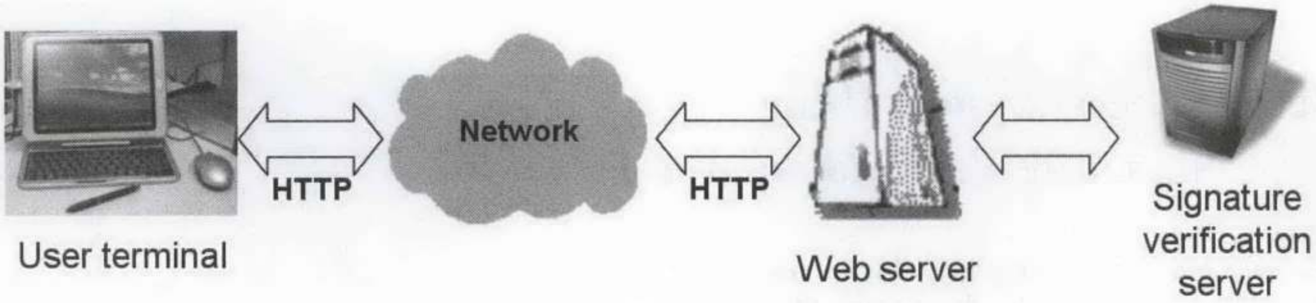


Fig. 1. Global architecture of the implemented prototype

Table 1. Applications of a network-based signature verification system

Applications	Example
e-banking	Access to bank account
e-commerce	Secure transactions in Internet
Login	Secure access to home/office computer, LAN, Web account, mobile telephone, laptop, PDA, etc.
POS (Point-of-Sale)	Secure payment with credit card, verifying customers before charging their credit cards
Physical Access Control	Secure access to restricted areas
Medical records management	Secure access to medical records. Only authorized users are allowed to get access
e-Government	Secure operations such as ID card or driver license renovation, income tax return submissions, etc.
Electronic data security	Access and encryption of sensitive data

need to ensure that only authorized terminals notify acceptation/rejection decisions.

USER ENROLMENT

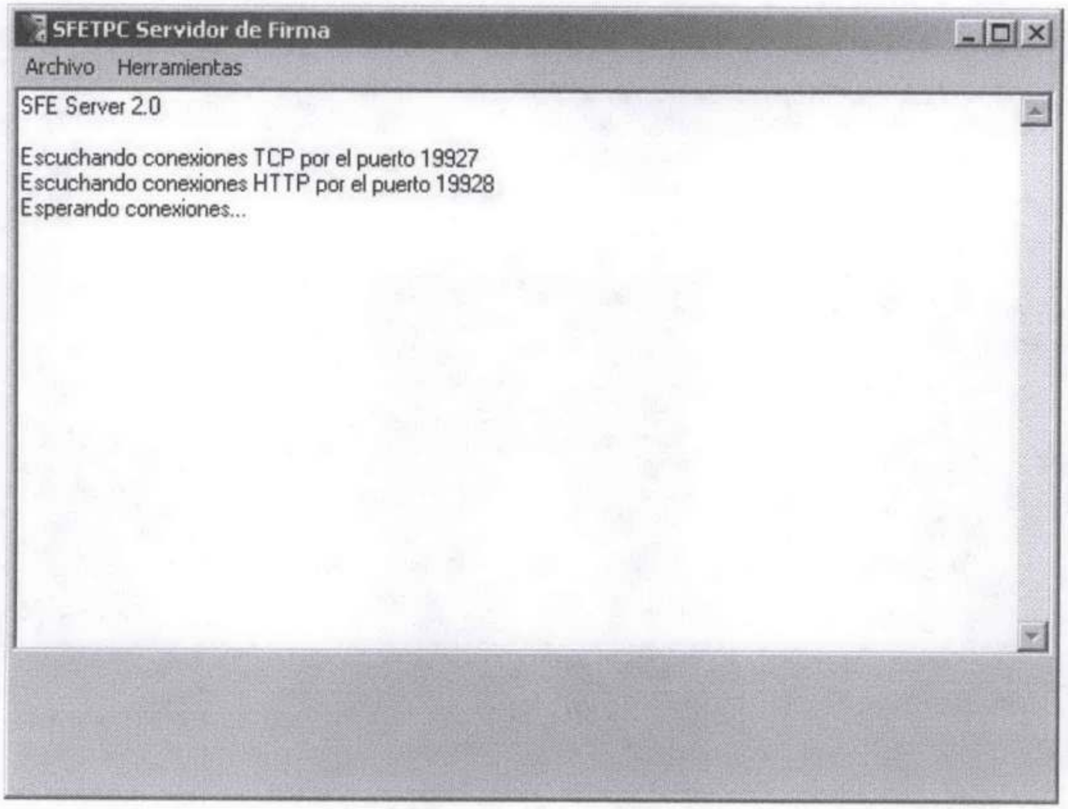
The next steps are performed in order to enroll a user in the system:

- The user is first authorized by an administrator in the signature verification server. A username and a temporary password are assigned to the user. This ensures that only desired users have authorization to use the signature-based verification system.
- Second, the user is requested to provide five signatures. These five signatures are used to generate a statistical model which characterizes the identity of the user [7]. The statistical model is generated in our prototype using the coordinate trajectories and pressure signals provided by the Tablet PC [5]. Technical details of the algorithm for statistical model generation can be found in [8, 9]. In our system, the user can provide its five signatures remotely with a downloadable application by using the temporary password assigned in the previous step. This scheme provides high flexibility. If a more secure environment is needed, another option is to enroll the users only in the presence of an administrator.

In order to account for the time variability of the signature signals, the five signatures used for enrollment are provided in two different sessions separated by a certain amount of time, typically 1 to 3 days. In addition, the statistical model of the user is updated along time by using the signature acquired in the last successful access.

THE SIGNATURE VERIFICATION SERVER

The signature verification server manages the verification process. It receives the requests for verification and decides if the user is accepted or not. In Figure 2 we can see the main window of our signature verification server. It shows the last



```
SFE Server 2.0

Escuchando conexiones TCP por el puerto 19927
Escuchando conexiones HTTP por el puerto 19928
Esperando conexiones...
```

Fig. 2. Main window of the signature verification server

transactions that have been realized, which are also stored on a log file. It also allows us to perform the following actions:

- *User authorization,* as described in the previous section.
- *User management.* The next information is available for each enrolled user: name, date of the last successful access, number of unsuccessful accesses since the last successful access, and block status. If a user accumulates a certain number of continuous unsuccessful accesses, he/she is blocked. In Figure 3 we can see the user management window.
- *System management.* This module has the following options: storage place of the user's data, unsuccessful accesses allowed to the users, communication settings of the signature verification server, storage place of the log file, rules for updating the statistical models of a user, etc.

It is supposed that only authorized administrators have access to the signature verification server.

USAGE OF THE WEB-BASED SECURE ACCESS CLIENT

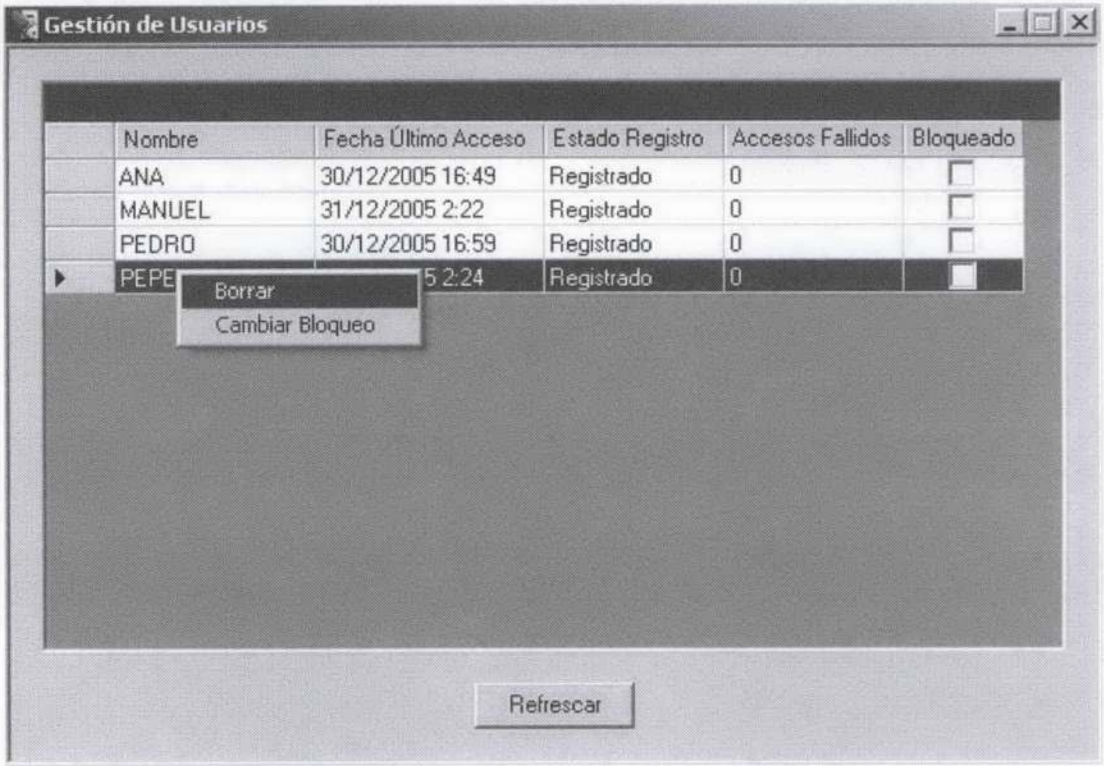
Once enrolled in the system, the user has access to the proper URL using its terminal. Figure 4 shows the main window of our prototype, where the username and a signature realization are requested. If the user is accepted, he/she will be allowed to access his account. If not, an appropriate message will indicate that he/she has been rejected.

SECURING A NETWORK-BASED SIGNATURE VERIFICATION SYSTEM

A discussion of issues and concerns related to the design of a secure fingerprint recognition system is addressed in [10]. Some of these concerns also apply in the case of signature verification systems.

When designing a recognition system, we have to decide whether it is going to operate in verification or identification mode [1]. In verification mode, an individual who desires to be recognized claims an identity, and the system compares the captured biometric data with the biometric template corresponding to the claimed identity. In identification mode, the system recognizes an individual by comparing the captured biometric data with the templates of all the users stored in the system. If the number of users is large, verification mode is recommended unless identification is strictly necessary.

Typically, developers and integrators of systems and applications are not the producers of hardware and core software. Several factors should be taken into account when choosing hardware and software components: choose proven hardware and software technology; check standards



Nombre	Fecha Último Acceso	Estado Registro	Accesos Fallidos	Bloqueado
ANA	30/12/2005 16:49	Registrado	0	□
MANUEL	31/12/2005 2:22	Registrado	0	□
PEDRO	30/12/2005 16:59	Registrado	0	□
PEPE	5 2:24	Registrado	0	□

Fig. 3. User management window of the signature verification server

compliance with platforms or operating systems; evaluate cost versus performance trade-off; ask for available support; etc. An SDK is usually supplied by the vendors, but system designers will usually have to develop specific applications for managing the enrollment, managing the storage and retrieval of templates and information, setting up the system options, etc.

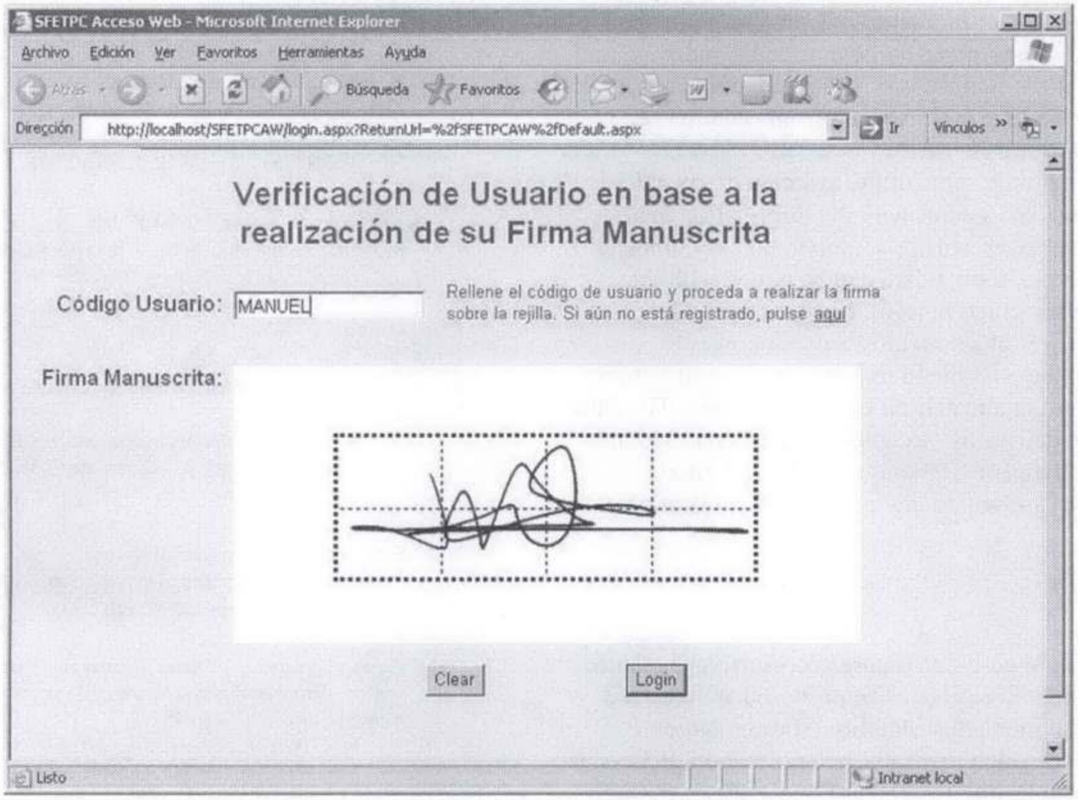
A policy of how to deal with users with bad quality signatures has to be defined. In signature-based verification this is related to users whose signature is easy to imitate. An attended enrollment can deal with this problem, forcing users to provide signatures which are not easy to imitate, but this may result in future false rejection alarms. It is said that the security of the entire system is only as good as the weakest "password," so users with simple signatures may compromise the security of the overall application.

System administration is an important issue. The administrator may instruct users and make them familiar with the signature acquisition device. He is also in charge of the state of the acquisition devices if the verification is made in a supervised scenario. Monitoring the system log is also an important task to find out if the system is being subjected to attacks. A threat model for the system has to be defined and the system has to be guarded against them. The threat model has to be based on what needs to be protected and from whom. The typical threats in a verification system are the following:

- *Denial of Service (DoS):* the system is damaged so legitimate users can no longer access it.
- *Circumvention:* illegitimate users gain access to the system.
- *Repudiation:* a legitimate user denies having accessed the system.
- *Covert acquisition*: trait samples of a legitimate user are obtained without his knowledge and subsequently used for illegitimate access.
- *Collusion:* illegitimate access by means of special super-users who are allowed to bypass the verification stage.
- *Coercion:* a genuine user is forced to access the system.

In Figure 5 we can see the main modules and dataflow paths in a signature verification system. The eight possible attack points marked are: 1) Scanner, 2) Channel between the scanner and the feature extractor, 3) Feature extractor, 4) Channel between the feature extractor and the matcher, 5) Matcher, 6) Database, 7) Channel between the database and the matcher, 8) Channel between the matcher and the application requesting verification.

Note that attacks 2, 4, 7, and 8 are launched against communications channels and are collectively called "replay" attacks. Signals in these channels can be intercepted and used at a later time. Attacks 1, 3, 5, and 6 are launched against system modules and are called Trojan horse attacks. A Trojan



SFETPC Acceso Web - Microsoft Internet Explorer

Dirección http://localhost/SFETPCAW/login.aspx?ReturnUrl=%2fSFETPCAW%2fDefault.aspx

Verificación de Usuario en base a la realización de su Firma Manuscrita

Código Usuario: MANUEL

Rellene el código de usuario y proceda a realizar la firma sobre la rejilla. Si aún no está registrado, pulse aquí

Firma Manuscrita:

Fig. 4. Main window of our Web-based secure access prototype

horse program can disguise itself as the module and bypass the true module, submitting false signals. For example, a Trojan horse program can perform a circumvention or denial-of-service (DoS) attack by always generating an acceptance or rejection decision in the matcher, respectively. Also, the sensor can be destroyed in a denial-of-service (DoS) attack.

It is very important that the feature extractor, matcher, and database reside at a secure and trusted location. The scanner should implement some security capabilities (e.g.: encryption). Also, a mechanism of trust should be established between the components of the system.

Mutual identification can be achieved by embedding a shared secret (e.g.: a key for a cryptographic algorithm) or by using a Certificate Authority (CA – an independent third party that everyone trusts and whose responsibility is to issue certificates).

PRIVACY ISSUES

Privacy is the ability to lead one's own life free from intrusions, to remain anonymous, and to control access to one's own personal information [2]. It is widely accepted that biometric identifiers provide positive person recognition better than conventional technologies (token-based or knowledge-based). But several arguments and objections are given against biometric recognition: hygiene of biometric scanners that require contact; negative connotations associated with some biometrics used in criminal investigation (DNA, fingerprint, face); inference of information from biological measurements; linkage of biometric information between different applications, allowing to track individuals, either with or without permission; acquisition of biometric samples without knowledge of the person, allowing covert recognition of

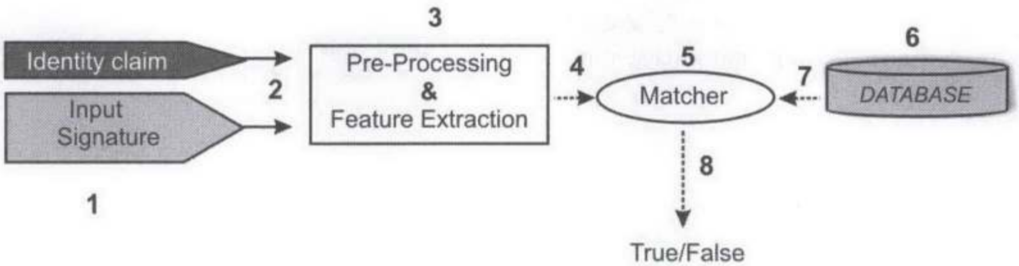


Fig. 5. Design of a signature verification system. The possible security attack points are marked with numbers from 1 to 8

people; etc. The abuse of biometric information is an open issue that should be addressed by governments, industry, and organizations. Unless a consensus is reached, citizens may be reluctant to provide biometric measurements and to use biometric recognition systems.

One way to deal with some of the associated privacy problems is the use of systems with the information in a decentralized place over which the individual has complete control. For example, a smartcard can be issued with the template of the user stored in it [6]. Even more, as the computational power of smartcards is continuously increasing, it will be possible to implement the verification step inside the card in a match-on-card architecture. The card will only have to deliver the accept/reject decision. In that case, neither the template of the user nor the acquired biometric samples are sent to any centralized application.

CONCLUSIONS

A prototype for Web-based secure access using signature verification has been described. The proposed architecture ensures high versatility and scalability. The signature verification server, which manages the verification process, is capable of communicating with a variety of sensors through several kinds of networks using standard protocols such as HTTP. It can be customized depending on factors such as: allowed number of users, cost of the acquisition sensors, network used in the access, storing or processing capacity of the signature verification server, etc.

Several issues have to be taken into account when designing a network-based signature verification system: mode of operation (verification or identification), selection of hardware and software components, policy with users with bad quality signatures, administration of the system, definition of a threat model, detection of attacks and implementation of a mechanism of trust between components of the system. Privacy issues have to be also considered when designing a system based on biometric information.

ACKNOWLEDGEMENTS

This work has been supported by BBVA, BioSecure NoE and the TIC2003-08382-C05-01 project of the Spanish Ministry of Science and Technology. F. A.-F. and J. F.-A. thank Consejeria de Educacion de la Comunidad de Madrid and Fondo Social Europeo for supporting their PhD studies.

REFERENCES

[1] A.K. Jain, A. Ross and S. Prabhakar,
An Introduction to Biometric Recognition,
IEEE Trans. on Circuits and Systems for Video Technology,
Vol. 14, No. 1, pp. 4-20, January 2004.

[2] S. Prabhakar, S. Pankanti and A.K. Jain,
Biometric Recognition: Security & Privacy Concerns,
IEEE Security & Privacy Magazine, Vol. 1, No. 2,
pp. 33-42, March-April 2003.

[3] R. Plamondon and S.N. Srihari,
On-line and off-line handwriting recognition: A comprehensive survey,
IEEE Transa. on Pattern Analysis and Machine Intelligence,
Vol. 22, No. 1, pp. 63-84, January 2000.

[4] M. Faundez-Zanuy,
Signature verification state-of-the-art,
IEEE Aerospace and Electronic Systems Magazine,
Vol. 20, No. 7, pp. 28-32, July 2005.

[5] F. Alonso-Fernandez, J. Fierrez-Aguilar and J. Ortega-Garcia,
Sensor interoperability and fusion in signature verification:
A case study using Tablet PC,
Proc. IWBRS, *Lecture Notes in Computer Science,*
Vol. 3718, pp. 180-187, October 2005.

[6] R. Sanchez-Reillo,
Smart card information and operations using biometrics,
IEEE Aerospace and Electronic Systems Magazine,
Vol. 16, No. 4, pp. 3-6, April 2001.

[7] J. Fierrez-Aguilar, Loris Nanni, J. Lopez-PeZalba, J. Ortega-Garcia and Davide Maltoni,
An on-line signature verification system based on fusion of local and global information,
Proc. AVBPA, *Lecture Notes in Computer Science,*
Vol. 3546, pp. 523-532, July 2005.

[8] J. Ortega-Garcia, J. Fierrez-Aguilar, J. Martin-Rello and J. Gonzalez-Rodriguez,
Complete signal modelling and score normalization for function-based dynamic signature verification,
Proc. AVBPA, *Lecture Notes in Computer Science,*
Vol. 2688, pp. 658–667, 2003.

[9] J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez,
Target dependent score normalization techniques and their application to signature verification
IEEE Trans. on SMC-C, Special Issue on Biometric Systems,
Vol. 35, 2005.

[10] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar,
Handbook of Fingerprint Recognition,
Springer, 2003.