Signature Verification on Handheld Devices

Marcos Martinez-Diaz, Julian Fierrez, Javier Galbally, Fernando Alonso-Fernandez, and Javier Ortega-Garcia

Biometric Recognition Group - ATVS, EPS - Univ. Autonoma de Madrid
C/ Francisco Tomas y Valiente, 11 - Campus de Cantoblanco - 28049 Madrid, Spain
{marcos.martinez, julian.fierrez, javier.galbally,
fernando.alonso, javier.ortega@uam.es

Abstract. Signature verification for handheld devices (e.g. smartphones, PDAs, etc.) as an authentication method is studied. Signature can be used to authenticate users in mobile networks for secure transactions. The challenges of signature verification on mobile devices are addressed and analyzed and the architecture for a verification platform is outlined. We propose a verification system adapted to handheld devices and study its performance. Results are given for the scenarios of casual and skilled impostors using a subcorpus of the BIOSECURE multimodal biometric database.

Key words: biometrics, signature verification, PDA, smart phone

1 Introduction

In our increasingly networked environment, secure access control and user authentication are common tasks which are usually performed with tokens or passwords. In this field, biometrics has become a focus of interest as it uses physiological (e.g. fingerprint, iris) or behavioral (e.g gait, signature) traits to authenticate a user [1]. These traits cannot be easily stolen in general (without severe consequences for the user) or forgotten. It is now common to observe fingerprint verification systems in handheld and portable electronic devices, face recognition systems for border control purposes and iris verification when accessing highly secured areas.

Among all biometric traits, signature is one of the most socially accepted as it has been used in financial and legal transactions for centuries. Despite its acceptance, automatic signature verification is still a challenging task. This can be corroborated by the variety of research works conducted in the last decades [2–4]. One of the main challenges in signature verification is related to the signature variability. While signatures from the same user show considerable differences between different captures (high *intra-class* variability), skilled forgers can perform signatures with high resemblance to the user's signature (low *inter-class* variability). Moreover, when a system is designed, only a fraction of information about skilled forgeries can be obtained as forgers with unexpected skills can appear at any time once the system has been deployed.

Fig. 1. Some currently available smartphones with writing enabled touchscreens. (From left to right: HP iPAQ hw6915, Sony Ericcson P1i and Nokia 7710)

Two main classes of signature verification systems exist. *Off-line* systems use static signature images, which may have been scanned or acquired using a camera, to perform verification. *On-line* or *dynamic* systems use captured signature time-functions. These functions are obtained using digitizer tablets or touchscreens (e.g. Tablet-PCs, smart phones, etc.). Traditionally, dynamic systems have presented a better performance than off-line systems as more levels of information than the signature static image are available [2].

Smart phones and other handheld devices represent a feasible platform for the deployment of a dynamic signature verification systems as they provide both a pen-based input and enough computing power (see Fig. 1). Smart phones have gathered an increasing interest among the scientific and industrial communities as they provide a convenient way of interfacing with other systems and can be consequently host a wide range of user-centric applications [5–7]. Verification of signatures in smart phones or other mobile devices provides a convenient method for user authentication in commercial payments or financial transactions among other applications.

In this work we consider dynamic signature verification on smart phones and mobile devices and overview its major applications and challenges. Additionally, we propose a verification system specifically adapted to handheld devices. The system is tested using a recently captured signature database on a PDA device under realistic conditions in the framework of the European Network of Excellence BIOSECURE [8]. The work is structured as follows: dynamic signature verification, its applications and challenges are introduced in Sect. 2, the proposed system is presented in Sect. 3 and conclusions are finally drawn in Sect. 4.

2 Dynamic Signature Verification

The architecture of a signature verification system is depicted in Fig. 2. Dynamic signature verification systems perform the following steps [4]:

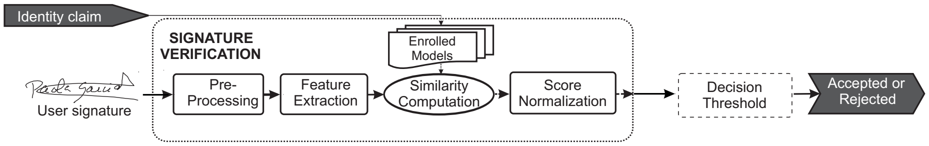


Fig. 2. Signature Verification System Architecture.

1. **Data Acquisition**: Signature signals are captured using a digitizing device or touchscreen as a PDA or Tablet-PC. The signature signal is sampled and stored as discrete time series. While some digitizing tablets provide pressure or pen angle information, these are not commonly available in handheld devices. Pre-processing tasks such as noise filtering and alignment may be carried out in this phase.
2. **Feature Extraction**: Two main approaches have been followed in this step: *feature-based* systems extract global features (e.g. signature duration, number of pen-ups, average velocity) from the signature in order to obtain a holistic feature vector. *Function-based* systems use the signature time functions (e.g. position, pressure) for verification.
3. **Enrollment**: In *model-based* systems a statistical user model is computed using a training set of genuine signatures which is used for future comparisons in the matching step. *Reference-based* systems store the features of each signature of the training set as templates. In the matching process the input signature is compared with each reference signature.
4. **Similarity Computation**: This step involves *pre-alignment* if necessary and a *matching* process, which returns a *matching score*. In feature-based systems, statistical techniques like Mahalanobis distance, Parzen Windows or Neural Networks are used for matching [9]. Function-based systems use other techniques like Hidden Markov Models (HMM) [10], or Dynamic Time Warping (DTW) [11] to compare signature models.
5. **Score Normalization**: The matching score may be normalized to a given range. More sophisticated techniques like target-dependent score normalization can lead to an improved system performance [12].

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

2.1 Applications of Signature Verification on Handheld Devices

Touch-screen enabled mobile devices such as smart phones or PDAs provide an appropriate computing platform for signature verification. In fact, commercial devices already provide handwritten character recognition as a text input alternative [6, 13].

Signature verification can be used for a wide range of applications. Among them, we cite the following:

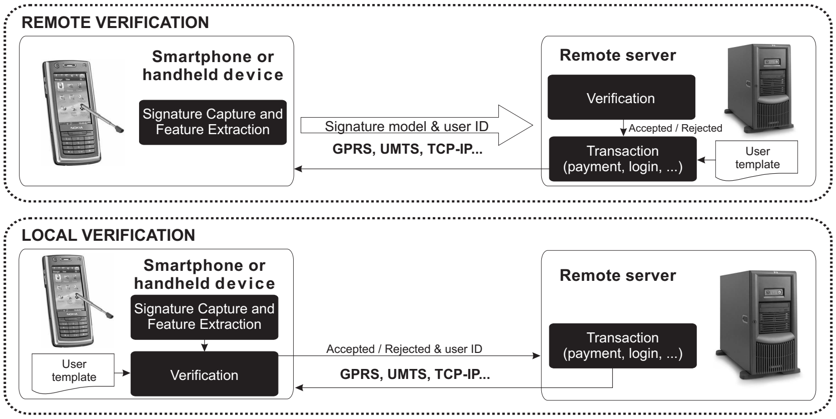

REMOTE VERIFICATION
Smartphone or handheld device
Signature Capture and Feature Extraction
Signature model & user ID
GPRS, UMTS, TCP-IP...
Remote server
Verification
Accepted / Rejected
Transaction (payment, login, ...)
User template
LOCAL VERIFICATION
Smartphone or handheld device
Signature Capture and Feature Extraction
User template
Verification
Accepted / Rejected & user ID
GPRS, UMTS, TCP-IP...
Remote server
Transaction (payment, login, ...)

Fig. 3. Diagram of two possible architectures of a dynamic signature verification platform for handheld devices (The verification steps have been simplified).

Payments in commercial environments: the signature is used to validate a payment that is performed via UMTS, GPRS, or other network. This means ubiquitous access to commercial transactions wherever a mobile network is available.

Legal transactions: legal documents or certificates are signed by the user adding additional security as the signature is verified. This can be a convenient user validation scheme for e-government applications.

User login: the signature is used to login into a local or remote system as an access control measure (e.g. bank account, personal records, etc.)

Client validation: A client is validated by its signature. A client that receives a service or a delivery (e.g. a parcel) signs in a mobile device carried by the deliverer or service provider.

Cryptobiometrics: Signature is used as a cryptographic key [14] that identifies the user.

In all these applications, the verification system can be either remote or local. Local verification systems perform the matching process in the handheld device, while remote systems send the input signature model over the network and matching is performed on a remote server. A model of the two aforementioned architectures is presented in Fig. 3. Security must be ensured in both architectures. While in local systems, the user template and matcher must be secured in the handheld device, in remote systems, the transmitted model and verification system on the server side must be kept secure.

A key advantage for the deployment of such systems is that touch-screen enabled mobile devices do not need any extra hardware for signature verification, as it is the case of fingerprint sensors or cameras for fingerprint and face verification systems respectively. Consequently, no extra costs exist and the system complexity does not increase.

2.2 Challenges of Signature Verification on Hanheld Devices

Signature Verification system designers must face many challenges. As has been previously stated, inter- and intra-variability represent one of the main difficulties when trying to reach a good verification performance, specially in the case of skilled forgeries.

Handheld devices such as smart phones or PDAs are affected by size and weight constraints due to their portable nature. While processing units, memory chips and battery components are nowadays experimenting higher levels of miniaturization and integration, the input (e.g. keyboard, touch-screen) and output (e.g. display) parts must have reasonable dimensions in order to keep their usability. Poor ergonomics and small input areas in mobile devices are two key factors that increase the variability during the signing process.

The touch-screen digitizing quality must also be taken into account. Irregular sampling rates and sampling errors, which are common in mobile devices, may worsen the verification performance and must be addressed during the preprocessing steps. In these devices, only position signals are available in general. Pressure, pen-azimuth or other signals that may improve the verification performance [4], are not usually available in handheld devices.

The interest in security on smart phones has raised in the last few years [15]. Security must be a critical concern while designing a signature verification platform as a breach could give an attacker access to personal data or bank accounts. Gaining access to the matcher could allow an attacker to perform software attacks such as brute force or hill-climbing attacks [16]. The user template must be appropriately secured and encrypted as well as communication channels over which signature information may be transmitted.

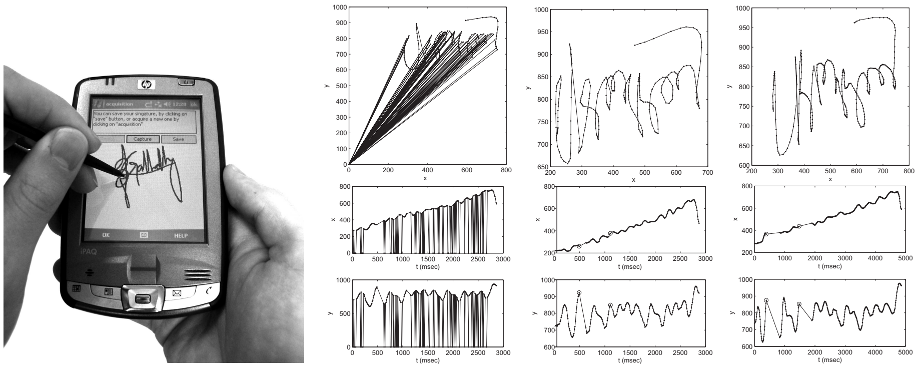
3 Signature Verification System

We propose a feature-based signature verification system. A set of 100 features is initially considered from each signature. Some examples of features are: signature duration, number of pen-ups, average velocity and direction histograms. A complete description of the features can be found in [9].

The SFFS feature selection algorithm [17] is used to select the subset of features that provide the best verification results for the handheld scenarios considered in the experiments. User models $C = (\boldsymbol{\mu}, \boldsymbol{\Sigma})$ are built from a training set of signatures. The matching score is obtained as the inverse of the Mahalanobis distance $d(\mathbf{x}, C)$ between the input signature feature vector $\mathbf{x}$ and the user model C.

3.1 Database and Experimental Protocol

A subset of the signature corpus of the BIOSECURE multimodal biometric database [18] is used. The subset consists of 50 users, with 20 genuine signatures and 20 skilled forgeries per user, leading to $50 \times (20 + 20) = 2000$ signatures.



(a) (b)

Fig. 4. (a) Signature capture process. (b) Example of signatures from a user of the database. From left to right: genuine signature without preprocessing, genuine signature and skilled forgery. Pen-ups are marked with circles in the x- and y-coordinate time series. The signatures from the picture and the graphs are from different users.

Genuine signatures are acquired in two different sessions separated by months, being 5 from the first and 15 from the second session. In each session, signatures are performed in blocks of 5, leaving a gap of some minutes between each block. Signatures are captured with an HP iPAQ 2790 PDA while the user is standing and holding the PDA with one hand. Only the x and y coordinates and sample timestamps are available. Skilled forgeries for each user are performed by 4 different users (5 forgeries each) in a “worst case” scenario, where each forger has access to the dynamics of the genuine signature and a tracker tool allowing to see the original strokes. User models are trained with 5 genuine signatures of the first session (all from the same block), leaving the remaining 15 signatures from the second session to compute genuine user scores.

An example of the capture process is shown in Fig. 4.a and examples of a genuine captured signature and a skilled forgery are shown in Fig. 4.b. Due to degraded capture conditions, a pre-processing step is first performed, where incorrectly detected samples (see Fig. 4.b, left column) are linearly interpolated. As no pen pressure information is provided, pen-ups are assigned wherever a gap of 50 or more milliseconds between two consecutive samples exist.

Random forgery scores (the case where the forger uses his own signature to claim being another user) are computed by comparing the user model to one signature of all the remaining users (leading to 50 × 49 random forgery scores). Skilled forgery scores are computed by comparing all the available skilled forgeries per user with its own model (leading to 50 × 20 scores).

The system performance is evaluated using the Equal Error Rate (EER). This rate is obtained by setting the matching threshold so that the False Acceptance Rate (FAR; the case where a forger is accepted as a user) and the False Rejection Rate (FRR; the case where a genuine user is rejected by the system) are equal.

Table 1. System performance for the three different scenarios.

Scenario	Random forgeries EER (%)	Skilled forgeries EER (%)
Random forger scenario	0.57	26.92
Skilled forger scenario	3.64	13.32
Mixed scenario	2.04	14.17

Three different scenarios are considered, depending on the type of forgeries that the system is focused on:

Random forger scenario: The feature selection step is set to optimize the performance in the case of random forgeries.

Skilled forger scenario: The feature selection step is set to optimize performance in the case of skilled forgeries.

Mixed scenario: The feature selection step is set to minimize the sum of the EER for skilled and random forgeries.

3.2 Results

The results of the three scenarios are shown in Table 1. As can be seen, the system performance varies remarkably for each scenario, which denotes that the most distinctive features for random forgeries and skilled forgeries differ substantially. Despite the moderately high error rates for skilled forgeries, the "worst case" nature of the forgeries, where users have access to complete information about the signing process suggests a lower error rate in real applications.

These results are very promising, as feature-based systems provide baseline performance that can be improved by combining them to other approaches based on complementary information [9].

4 Conclusions and Future Work

The feasibility of dynamic signature verification as a user-centric validation service on mobile devices has been studied. Signature verification allows to perform ubiquitous user validation with a wide range of commercial, legal and security applications. The challenges and applications of signature verification on such devices were addressed and the architecture of a user verification system based on signature verification and mobile devices has been outlined. As a case study, a signature verification system adapted to mobile conditions is presented and its performance using a database captured on a PDA has been analyzed.

The proposed verification system has shown very promising results, which can be enhanced by its fusion with other approaches proposed in the literature.

While signature verification is still a challenging task, the performance of the systems is being continually improved with new approaches and algorithms. Moreover, the combination of signature with other biometric traits can lead to very low error rates [19]. This is feasible in camera- or fingerprint sensor-enabled handheld devices, which can perform face or fingerprint verification.

Acknowledgments. This work has been supported by the Spanish Ministry of Education under project TEC2006-13141-C03-03 and by the European Network of Excellence Biosecure (IST-2002-507634). J. Fierrez is supported by a Marie Curie Fellowship from the European Commission.

References

1. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: A tool for information security. IEEE Trans. on Information Forensics and Security **1**(2) (2006) 125–143
2. Plamondon, R., Lorette, G.: Automatic signature verification and writer identification: The state of the art. Pattern Recognition **22**(2) (1989) 107–131
3. Plamondon, R., Srihari, S.N.: On-line and off-line handwriting recognition: A comprehensive survey. IEEE Trans. on Pattern Analysis and Machine Intelligence **22** (2000) 63–84
4. Fierrez, J., Ortega-Garcia, J.: On-line signature verification. In: Handbook of Biometrics. Eds. A. K. Jain and A. Ross and P. Flynn (in press) (2007)
5. Iftode, L., Borcea, C., Ravi, N., Kang, P., Zhou, P.: Smart phone: an embedded system for universal interactions. In: Proc. of 10th IEEE Intl. Workshop on Future Trends of Distributed Computing Systems, FTDCS. (2004) 88 – 94
6. Ballagas, R., Borchers, J., Rohs, M., Sheridan, J.: The smart phone: a ubiquitous input device. IEEE Pervasive Computing **5**(1) (2006) 70–77
7. Roussos, G., Marsh, A., Maglavera, S.: Enabling pervasive computing with smart phones. IEEE Pervasive Computing **4**(2) (2005) 20–27
8. Biosecure Network of Excellence: Biosecure multimodal database (2007) (http://www.biosecure.info).
9. Fierrez-Aguilar, J., Nanni, L., Lopez-Penalba, J., Ortega-Garcia, J., Maltoni, D.: An on-line signature verification system based on fusion of local and global information. In: Proc. of IAPR Intl. Conf. on Audio- and Video-Based Biometric Person Authentication, AVBPA, Springer LNCS-3546 (2005) 523–532
10. Fierrez, J., Ortega-Garcia, J.: Function-based on-line signature. In: Advances in Biometrics: Sensors, Systems and Algorithms. Springer (2007)
11. Kholmatov, A., Yanikoglu, B.: Identity authentication using improved online signature verification method. Pattern Recognition Letters **26**(15) (2005) 2400–2408
12. Fierrez-Aguilar, J., Ortega-Garcia, J., Gonzalez-Rodriguez, J.: Target dependent score normalization techniques and their application to signature verification. IEEE Trans. on Systems, Man and Cybernetics, part C **35**(3) (2005) 418–425
13. Anquetil, E., Bouchereau, H.: Integration of an on-line handwriting recognition system in a smart phone device. In: Proc. of 16th Intl. Conf. on Pattern Recognition, ICPR. Volume 3. (2002) 192–195
14. Freire-Santos, M., Fierrez-Aguilar, J., Ortega-Garcia, J.: Cryptographic key generation using handwritten signature. In: Proc. SPIE. Volume 6202. (2006) 225–231
15. Khokhar, R.: Smartphones a call for better safety on the move. Network Security **2006**(4) (2006) 6–7
16. Galbally, J., Fierrez, J., Ortega-Garcia, J.: Bayesian hill-climbing attack and its application to signature verification. In: Proc. IAPR Intl. Conf. on Biometrics, ICB, Springer LNCS (2007)
17. Pudil, P., Kittler, J.N.J.: Flotating search methods in feature selection. Pattern Recognition Letters **15** (1994) 1119–1125
18. Faundez-Zanuy, M., Fierrez-Aguilar, J., Ortega-Garcia, J., Gonzalez-Rodriguez, J.: Multimodal biometric databases: An overview. IEEE Aerospace and Electronic Systems Magazine **21**(8) (August 2006) 29–37
19. Ross, A., Nandakumar, K., Jain, A.K.: Handbook of Multibiometrics. Springer (2006)