On-line signature recognition through the combination of real dynamic data and synthetically generated static data

Article *in* Pattern Recognition · September 2015

DOI: 10.1016/j.patcog.2015.03.019

6 authors, including:

Javier Galbally
European Commission
86 PUBLICATIONS **842** CITATIONS
SEE PROFILE

Marta Gomez-Barrero
Darmstadt University of Applied Sciences
29 PUBLICATIONS **76** CITATIONS
SEE PROFILE

Aythami Morales
Universidad Autónoma de Madrid
69 PUBLICATIONS **398** CITATIONS
SEE PROFILE

Julian Fierrez
Universidad Autónoma de Madrid
243 PUBLICATIONS **3,994** CITATIONS
SEE PROFILE

Pattern Recognition 48 (2015) 2921–2934

Contents lists available at ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

On-line signature recognition through the combination of real dynamic data and synthetically generated static data

Javier Galbally [a,*], Moises Diaz-Cabrera [b], Miguel A. Ferrer [b], Marta Gomez-Barrero [a], Aythami Morales [a], Julian Fierrez [a]

[a] ATVS-Biometric Recognition Group, EPS, Universidad Autonoma de Madrid, Spain
[b] Instituto Universitario para el Desarrollo Tecnológico y la Innovación en Comunicaciones, Universidad de las Palmas de Gran Canaria, Spain

ARTICLE INFO

Article history:
Received 17 March 2014
Received in revised form
6 February 2015
Accepted 23 March 2015
Available online 3 April 2015

Keywords:
On-line signature verification
On-line and off-line signature fusion
Signature synthesis
Off-line signature verification
Biometric performance evaluation

ABSTRACT

On-line signature verification still remains a challenging task within biometrics. Due to their behavioural nature (opposed to anatomic biometric traits), signatures present a notable variability even between successive realizations. This leads to higher error rates than other largely used modalities such as iris or fingerprints and is one of the main reasons for the relatively slow deployment of this technology. As a step towards the improvement of signature recognition accuracy, the present paper explores and evaluates a novel approach that takes advantage of the performance boost that can be reached through the fusion of on-line and off-line signatures. In order to exploit the complementarity of the two modalities, we propose a method for the generation of enhanced synthetic static samples from on-line data. Such synthetic off-line signatures are used on a new on-line signature recognition architecture based on the combination of both types of data: real on-line samples and artificial off-line signatures synthesized from the real data. The new on-line recognition approach is evaluated on a public benchmark containing both real versions (on-line and off-line) of the exactly same signatures. Different findings and conclusions are drawn regarding the discriminative power of on-line and off-line signatures and of their potential combination both in the random and skilled impostors scenarios.

1. Introduction

Among the different biometric traits that have been proposed and studied in the literature, automatic handwritten signature verification stands out as one of the most attractive due to its social and legal acceptance, derived from the widespread use that has traditionally been given as a personal authentication method. In addition, handwritten signature also presents the appealing feature of being easily acquired either with an inking pen over a sheet of paper or by electronic means with a number of existing pointer-based devices (e.g., pen tablets, PDAs, mobile phones, and touch screens). As a consequence, signature recognition has been a very consistent and active field of research over the last three decades, with multiple works being published in this lapse of time. All these research efforts have been compiled in a number of comprehensive surveys that give a clear overview of the state of the art evolution from the first pioneering works in the 80 s to date [1–6].

However, in spite of its advantages, the practical deployment of this technology has been slower than what was foreseen some years ago, as its performance remains a step behind other largely used traits like fingerprint or iris. Such a poorer performance is mainly explained by three aspects that are typical of behavioural biometrics (i.e., biometric traits that we *learn* to produce): (i) due to its behavioural nature, the intra-class variability (i.e., difference among samples of the same individual) is in general higher than that of physiological biometrics (i.e., traits we are *born* with); (ii) also, learned traits such as the signature present a relatively low permanence over time, which decreases the accuracy of recognition systems [7]; (iii) finally, the fact that a signature is something that we can *learn* to produce opens two different impostor scenarios:

- *Random impostors*, also known as zero-effort impostors, are common to all biometrics, and refer to the case where the attacker tries to access the verification system with his own trait, while claiming a different user's identity. This is the most usual operating scenario defining the baseline performance of applications related to areas such as access control or

* Corresponding author.
E-mail addresses: javier.galbally@uam.es (J. Galbally), mdiaz@idetic.eu (M. Diaz-Cabrera), mferrer@idetic.eu (M.A. Ferrer), marta.barrero@uam.es (M. Gomez-Barrero), amorales@idetic.eu (A. Morales), julian.fierrez@uam.es (J. Fierrez).

http://dx.doi.org/10.1016/j.patcog.2015.03.019
0031-3203/

commercial transactions. As such, biometric verification systems are almost in all cases tuned to achieve a certain required performance in this scenario (i.e., the decision threshold is fixed considering random impostors).

- *Skilled impostors*: this scenario is unique for behavioural biometrics. This type of traits allows a different person to learn how to produce the genuine user's biometric identifier (e.g., the signature). In this scenario, the attacker has some knowledge of the genuine trait and tries to access the system imitating it. Such skilled forgeries usually lie inside the subject's intraclass variability leading to a significant decrease of the recognition performance. This operational framework is specially relevant in forensic related applications (e.g., signature forgery detection in checks or official documents).

The previous three behavioural-related aspects turn automatic verification of the handwritten signature into a very challenging research area. Such authentication task may be divided into two different but related modalities, according to the input information available: (*i*) *On-line* or *dynamic* signature recognition, which is based on the time functions produced during the signing process (e.g., position trajectories or pressure versus time), acquired using devices like touch screens or digitizing tablets; and (*ii*) *off-line* or *static* signature recognition, based on the static image of the signature, usually digitalized from a hard copy document.

Traditionally, on-line signature has been regarded as more accurate than its off-line version due to the greater amount of information available [6]. As already pointed out, off-line verification is based mainly on the geometric characteristics of the signature, while for the dynamic problem recognition algorithms can use not only the geometry but also *how* this geometry was generated and, therefore, should yield better performance rates. However, in the case of dynamic signature some information, such as the grey level distribution, the ink deposition model, or the geometric dependencies, could be difficult to exploit. Consequently, it is reasonable to assume, as it has already been shown in different works [8], that the optimal scenario in terms of recognition accuracy is to perform authentication based on both versions of the same signature (dynamic and static) and not on just one of them.

Unfortunately, in real applications this is very rarely the case, since the simultaneous acquisition of dynamic and static instances from the same signature is considerably time consuming, essentially due to the postprocessing steps required by off-line samples (e.g., digitalization and segmentation of the image). Due to these practical impediments, and in spite of their superior performance, fusion recognition approaches based on dynamic and static data have been largely neglected. As a consequence, for most real-time authentication applications, research has been focused on dynamic signature recognition thanks to its simple and fast automatic acquisition and its higher recognition performance compared to its off-line counterpart.

In the present work, we propose a novel strategy to overcome the above-mentioned reality, i.e. non-availability of both on-line and off-line versions of the same signature for recognition purposes. In particular, we describe a new method for the synthetic generation of static samples from their real dynamic instances. This method allows us to incorporate certain on-line information from the real signature (e.g., the speed, the pressure or the pen-ups trajectory), to the synthetic static image in order to increase its discriminative power specially in the presence of skilled forgeries. Then, synthetically generated off-line data are used within a novel on-line recognition architecture to enhance the performance of current top-ranked dynamic signature verifiers, comparing the accuracy of the new proposed approach with traditional fusion techniques based only on *real* data.

Such a study has been motivated by three facts, already highlighted above, which may be observed in the current general signature context in biometrics, namely

- Signature performance rates are still below the accuracy demanded by industry for many real-world applications and, therefore, new improved recognition algorithms and approaches are required.
- There is still not enough understanding of the relationship between on-line and off-line handwritten data and their potential synergy.
- Although some studies already exist both on on-line and off-line synthetic signature generation [9–11], the potential applications of synthetic biometric data are still largely unexplored.

With the previous motivations in mind, the questions raised in the present article include the following: under the experimental setup considered in the work, does the on-line modality outperform off-line recognition systems? Although both types of data (static and dynamic) are extracted from the same signature, what is their level of complementary? Can the fusion of both types of systems improve the best overall individual performance? Is it possible to generate synthetic off-line data from real dynamic signatures which improve the performance of the on-line based systems? How does synthetic off-line signature perform compared to real off-line data? Does the synthetic generation of off-line data allow creating enhanced signature static images in terms of their recognition performance? What other advantages can be obtained through the synthetic generation of off-line data from real on-line signatures?

The main objectives and contributions of the present work are directly derived from the previously raised questions and may be summarized as follows:

- Performance comparison on the exact same public benchmark (i.e., database and evaluation protocol) of top ranked state of the art on-line and off-line systems, both in the random and skilled-forgery scenarios. This way, valuable findings are extracted regarding the accuracy of both modalities.
- Analysis of the complementarity of on-line and off-line signature both in the random and skilled-forgery scenarios.
- Development and analysis of a dynamically enhanced method for the automatic generation of synthetic off-line data from real on-line signatures.
- Proposal of a new on-line signature recognition architecture based on the combination of real dynamic data and automatically generated synthetic off-line data (from those same real on-line samples).

The rest of the paper is structured as follows. A summary of the closest related works is given in Section 2. The novel approach for the generation of enhanced synthetic off-line signatures from on-line data is described in Section 3. The experimental protocol including databases, recognition systems and tests is presented in the following two sections, Sections 4 and 5. Validation and experimental results, as well as the new proposed on-line recognition architecture are given in Section 6. Conclusions are finally drawn in Section 7.

2. Related work

The present research work is related to a number of different areas within signature biometrics such as on-line and off-line monomodal signature verification [4,5] or synthetic handwritten signature generation [10,12,13]. Each of these fields presents a

solid research background with multiple studies impossible to cover here extensively. For this reason, the current section only refers to those works which are thematically closer to the objectives mentioned in Section 1. In particular, we will focus on past research which addresses the direct comparison of on-line and off-line signature verification performance and the feasibility of combining them in order to improve their overall recognition accuracy. Accordingly, other works that may be found in the literature which exploit certain common features between dynamic and static samples with different goals such as improving off-line signature segmentation [14], or aiding off-line signature recognition based on previous on-line enrolment [15], will not be covered here.

The fusion of static and dynamic signature to enhance the performance of automatic recognition systems has already been studied in several works, where it has been shown that such a fusion approach can yield a significant decrease in the error rates [8,16–18]. Although all of them represent very valuable research efforts, in most of these previous approaches, experiments are carried out on small proprietary databases which do not contain real off-line data (static signatures are generated as single stroke images from the on-line version) or where on-line and off-line samples were not acquired simultaneously but on different sessions. This way, such studies rely on experimental protocols where both versions (static and dynamic) of the exact same signatures are not available. In the present work all validation experiments have been carried out on the same public benchmark which comprises the on-line and off-line information for the same signatures of 132 users.

One of the first efforts that considered the combination of on-line and off-line features was conducted in [18]. The tests were carried out over a very limited database comprising 20 signatures per subject of 14 individuals. As many as 16 of those signatures were used to train user specific classifiers based on Hidden Markov Models (HMM). Only 40 skilled forgeries and 20 random forgeries were considered in the experiments. Although this work set the path for later research on on-line and off-line signature performance comparison, it does not strictly study the fusion of both types of systems, but rather analyses the complementarity of different static- and dynamic-based sets of features extracted from on-line samples. Competitive results were achieved in the work after combining the static and dynamic descriptors with a relative performance increase of around 3% with respect to the best individual feature set. Such a feature-based strategy was later followed in the literature by more comprehensive studies [19,20].

The first work that effectively studied the potential fusion between on-line and off-line signature verification systems was reported in [16]. The authors used a proprietary database captured with a digitizing tablet to analyse the performance of (i) an on-line verifier based on the pressure, pen-ups and total duration of the signature; and (ii) an off-line authentication system based on a feature vector extracted applying 1D-Log Gabor wavelets and Euler numbers. Then, score level fusion of the two approaches was applied, reporting a small performance improvement of around 1% with respect to the best monomodal system. One of the limitations of this study is that no off-line real data was acquired. All static samples were synthetically generated as simple single stroke images from the on-line versions. Therefore, it is not possible to establish a fair comparison between the performance of real and synthetic off-line signatures or whether their fusion with the dynamic data yields similar results.

In [17] the authors also analyse the benefits of combining static- and dynamic-based classifiers. However, no real off-line signatures are used in the experiments. As in the previous case, in this work the on-line signature is converted into a simple static image from which two rotation and scaling invariant features were extracted: the Normalized Fourier Descriptors (NFD) and the Normalized Central Moment (NCM). The speed signal was used to model the on-line sample. The authors claim that the combination of the three descriptors (speed, NFD and NCM) using a one hidden-layer perceptron, achieved an error rate of 0%, on the random forgery scenario evaluated over a proprietary database of 100 users with 10 repetitions per signer. The skilled forgery scenario was not considered.

Probably the most comprehensive work published to date in the field of on-line and off-line signature fusion was reported in [8]. In this case, experiments are carried out on a subset of the BiosecurID database which contains both on-line and off-line versions of the same samples for 132 users with 16 genuine signatures and 12 skilled forgeries per signer [21]. Different enrolment scenarios are considered (with four and 12 signatures, respectively) where it is shown that the combination of both modalities clearly outperforms the individual results, with an average relative improvement of around 50%, which is specially significant for the skilled forgeries case.

3. Enhanced off-line signature generation from dynamic signature sequences

The present section describes the new method for the generation of "dynamically enhanced" synthetic off-line signatures. The proposed technique will be evaluated later in Section 6 and used to improve the overall performance of on-line recognition systems.

The basis behind this novel approach and the contribution with respect to other previously proposed methods [10,11] is the integration of on-line information not present in regular static signatures (e.g., pressure, speed or trajectory during pen-ups), in order to produce enriched synthetic off-line samples that are expected to be more discriminative than those obtained by simply linking the dynamic trajectory points.

Although other signals such as the azimuth and elevation angles of the input pen might be taken into account, in this work we consider that an on-line signature is defined by three time sequences $\{x_t[m], y_t[m], p_t[m]\}$, specifying, respectively, the x and y coordinates, and the pressure applied during the signing process at the time instants $m = 1, \ldots, M$. Azimuth and elevation are discarded for two main reasons: (i) not all acquisition sensors capture these signals (e.g., usually mobile or hand-held devices such as tablets or smart phones do not detect them); (ii) these functions usually present a high level of intravariability and their use for signature recognition purposes is at least unclear [19].

The whole generation approach is illustrated in Fig. 1, where it can be seen that the method takes as input an on-line signature (defined by the sequences x_t, y_t and p_t) and returns as output a synthetic off-line signature defined by two images: (*i*) $I_{enhanced}$, which embeds in its grey level distribution and its stroke thickness, pressure and speed information contained in the original on-line signature; and (*ii*) $I_{pen-ups}$, which is generated from the trajectory information captured by the on-line digitizing device when the pen is not in contact with the paper.

The different successive steps included in the generation process of each of the two synthetic static images, $I_{enhanced}$ and $I_{pen-ups}$, are described in the following sections.

3.1. Scaling and interpolation

Real dynamic signatures are usually captured with digital devices such as tablets, smart-phones or PDAs, which generate discrete time sequences (i.e., x_t, y_t, p_t). On the other hand, real static signatures are acquired with commercial scanners that produce images defined in the 2-D spatial domain ($I(x, y)$). Therefore, some pre-processing of the

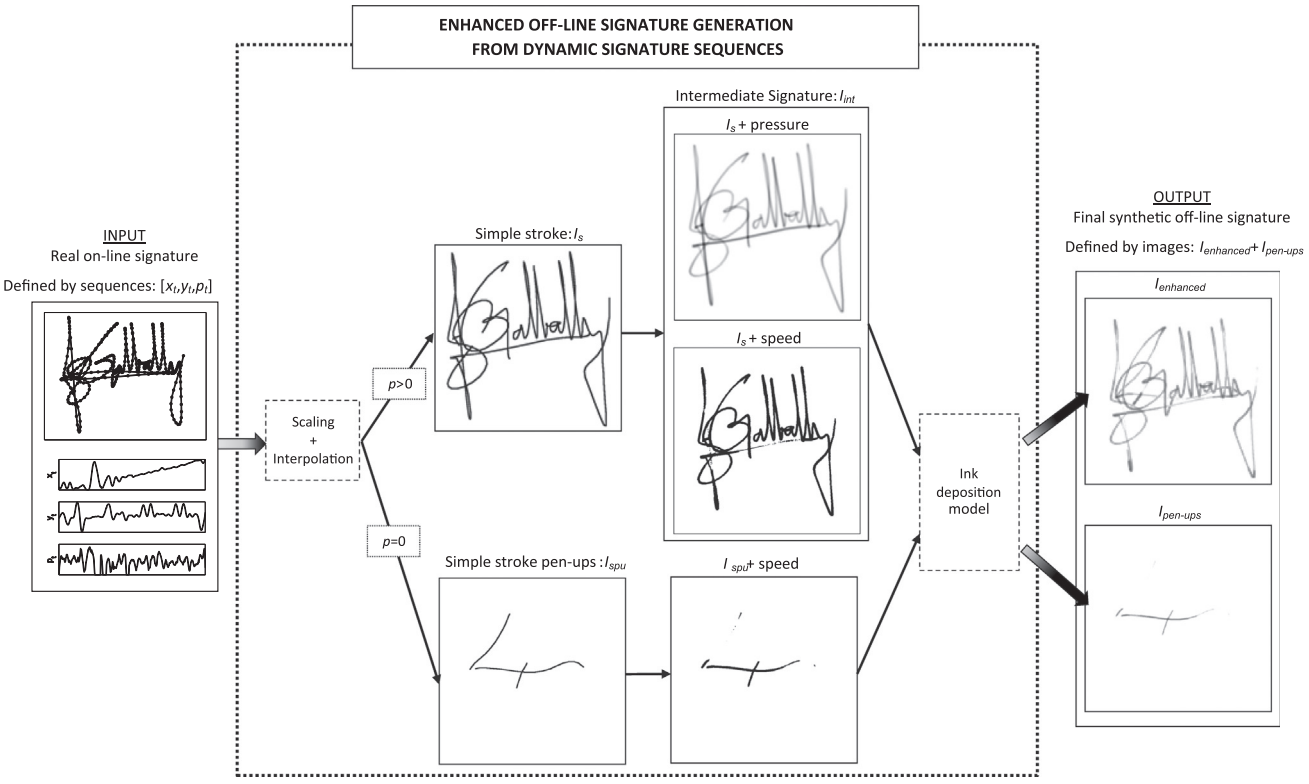

Fig. 1. Diagram of the enhanced off-line signature generation approach used in the work and described in Section 3.

real on-line data is required to be able to generate synthetic off-line images compatible with the real ones. In particular

- *Scaling*: In the present work, real off-line signatures were scanned at $R_{Scan} \sim 600$ dpi (see the database description in Section 4.1). On the other hand, the on-line acquisition device used in the acquisition had a resolution of $R_{Tab} \sim 2540$ dpi. Therefore, in order to generate synthetic off-line samples with the same resolution as the real static data, on-line coordinates are scaled by a factor $\kappa = R_{Scan}/R_{Tab}$.
- *Interpolation*: Since static signatures are continuous, the scaled discrete time on-line sequences (x_t, y_t, p_t) are linearly interpolated using Bresenham's line algorithm to obtain 8-connected sequences of length L: $\{x_c[n], y_c[n], p_c[n]\}_{n=1}^{L}$.

3.2. Enhanced static signature image: $I_{enhanced}$

In order to obtain the signature initial simple-stroke image (I_s in Fig. 1), the scaled and interpolated coordinate sequences, $\{x_c[n], y_c[n]\}_{n=1}^{L}$, are plotted on a white background for $\{p_c[n]\}_{n=1}^{L} > 0$ resulting in a black and white bitmap image.

The enhanced signature image is obtained by convolving each pixel from the simple-stroke image with a specific kernel. These kernels model the pen-tip spot at the different pixels using a different 2-D Gaussian for each pixel.

Let us define the sequence of images $\{I_n(x,y)\}_{n=1}^{L}$ as follows:

$$I_n(x,y) = \begin{cases} 1 & \text{if } (x \equiv x_c[n]) \text{ and } (y \equiv y_c[n]) \text{ and } (p_c[n] > 0) \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Then, the intermediate static signature I_{int} (see Fig. 1) is computed as

$$I_{int}(x,y) = \sum_{n=1}^{L} I_n(x,y) * G_n(x,y), \quad (2)$$

where $G_n(x,y)$ is defined as the following 2-D Gaussian function:

$$G_n(x,y) = A[n] \cdot \exp\left(-\left(\frac{x^2}{2\phi_x[n]} + \frac{y^2}{2\phi_y[n]} \right) \right). \quad (3)$$

This Gaussian function comprises the pressure and speed information from the on-line signature as follows:

- *Pressure information*: The Gaussian amplitude is computed as $A[n] = p_c[n] \cdot \Delta p + p_{min}$, where Δp and p_{min} are parameters to normalize $A[n]$ in the range [0.2–2.2]. Such normalization margin has been empirically selected in order to allow a wide range of grey-scale values related to the pressure signal, while avoiding any loss of information (i.e., grey points normalized to white) that could be potentially produced by a null Gaussian amplitude (for instance in the case of selecting a normalization range [0–1]).
- *Speed information*: One of the most discriminant on-line features is the signing time, which depends on the speed and the signature length. The horizontal and vertical speed functions (v_{xt}, v_{yt}) can be obtained as the first derivative of the original coordinate signals (x_t, y_t), with $v_{xt}[1] = v_{yt}[1] = 0$. As described in Section 3.1, the speed signal is then linearly interpolated to obtain $\{v_{xc}[n], v_{yc}[n]\}_{n=1}^{L}$.
  Signature strokes are directly affected by speed: The higher the signing speed, the thinner the strokes become. To approximate this concept, the speed information is introduced in the 2-D

Gaussian changing the blob width as part of the standard deviations ($\phi_x[n], \phi_y[n]$). When these standard deviations (spread of the elliptical blob) take high values, the spot width is enlarged (i.e., corresponding to low speed). On the other hand, the width becomes narrower for low values of the standard deviations (i.e., high speed). Such standard deviations are defined as

$$\left[\phi_x[n], \phi_y[n]\right] = \frac{\phi_{pen} \cdot R_{Scan}}{\delta} \cdot \left[\cos\left(v_{nx}[n]\right), \cos\left(v_{ny}[n]\right)\right] \quad (4)$$

where

$$\left[v_{nx}[n], v_{ny}[n]\right] = \frac{\pi/2}{\max_n\left(\{v_{xc}[n], v_{yc}[n]\}\right)} \cdot \left[v_{xc}[n], v_{yc}[n]\right] \quad (5)$$

R_{Scan} is defined as the spatial resolution of the static images (600 dpi in this work, as described in Section 3.1), δ is the conversion factor from mm to inches ($\delta = 2.54$) and ϕ_{pen} is empirically fixed to 3 mm in order to highlight the speed effect in the stroke. Given the equations above, it is possible to have null standard deviations, i.e. $(\phi_x[n], \phi_y[n]) = 0$, which lead to some points in the signature with no width. To avoid such situation, for those points in which $[\cos(v_{nx}[n]), \cos(v_{ny}[n])] = 0$, the value of the cosine is substituted by $\epsilon = 10^{-6}$.

Although both modulations, pressure (i.e., stroke grey level) and speed (i.e., stroke width), are applied at the same time through the use of G, for illustrative purposes, the two effects have been depicted separately in Fig. 1 (see diagrams "I_s+pressure" and "I_s+speed").

After the pressure and speed information have been included in the synthetic sample I_{int}, a virtual viscous ink profile is applied to produce the final image $I_{enhanced}$ (see Fig. 1). It is based on the overlapping of each consecutive individual spot so as to make them correspond to the rolling action of the ballpoint pen. Then, the histogram of the virtual trajectory is equalized to a real histogram of viscous ink. A similar approach is described in [11], in order to obtain a final realistic output in terms of the stroke texture.

3.3. Pen-ups static signature image: $I_{pen-ups}$

On-line devices are usually able to recognize the movement of the pen tip when it is close to the device, even if it is not in contact with the writing surface. This contactless movement is known as the pen-up trajectory, and corresponds to the time sequences when the pressure is null.

Since the pen does not deposit ink during pen-ups, they are not depicted in real static signature images. These trajectories, however, present some discriminative features that could be exploited in the skilled forgeries scenario, as impostors tend to imitate the inked image omitting the non-visible pen-up trajectory. The use of this information in off-line signature verification could therefore improve the accuracy of static synthetic signatures compared to their real versions, at a low computational cost.

The pen-up trajectory can either be added to $I_{enhanced}$, or generated as a new image. Given the relevance of pen-up information and that its combination with the inked strokes could occlude its discriminative ability (in general pen-up strokes are much shorter than inked ones), a new image with just the pen-ups is generated, $I_{pen-ups}$.

As a first step, an initial simple stroke pen-ups image I_{spu} is generated considering only the values $\{x_c[n], y_c[n]\}_{n=1}^{L}$ where $\{p_c[n]\}_{n=1}^{L} = 0$, after the scaling and interpolation process.

Then, this initial image I_{spu} is transformed following a similar process to that described in Section 3.2 to generate $I_{enhanced}$. However, in this case the Gaussian function G presents an amplitude $A[n]$ equal to one (independent of the pressure signal), so that only the stroke width is modulated according to the speed information, while the grey level remains constant.

Finally, the same ink deposition model as in the case of $I_{enhanced}$ is applied, resulting in a new image $I_{pen-ups}$, which takes advantage solely of the trajectory and the dynamic information found in pen-ups.

4. Databases and recognition systems

To fulfil the objectives set in the introduction of the present article, two databases of on-line and off-line signatures as well as three state of the art signature recognition systems are used. Both, databases and systems, are described next.

4.1. On-line and off-line signature databases: Real and synthetic

Two complementary databases are used in the experimental protocol: (i) a *real* database containing on-line and off-line versions of the exact same signatures, and (ii) a *synthetic* database of off-line signatures generated according to the method described in Section 3 based on the dynamic signatures of the real database.

As *real* evaluation database a subcorpus of the signature data in the BiosecurID multimodal database was used. BiosecurID was acquired in five different Spanish universities and comprises eight different biometric traits of 400 users captured in four sessions over a six month time span [21].

Handwritten signatures were acquired with the Intuos3 A4/Inking pen tablet placing a predefined paper template over the digitizing device as shown in Fig. 2. The users were told to sign inside a delimited grid in order to reduce the rotation and size variations (25 mm × 120 mm). Signatures were performed on the marked area with a special inking pen which also captured the x and y trajectories and the pen pressure during the signing process, with a sampling frequency of 100 Hz. This way, both versions, dynamic and static, of the same samples were captured *simultaneously*. In order to obtain the final off-line digitized samples, the grid-templates used to capture the static signatures were scanned at 600 dpi into png grey level files, which were then processed to automatically segment the signature images, stored with the same codename as their on-line versions.

Consequently, the database contains the off-line (on paper) and on-line versions of the *exact same* real signatures. This characteristic makes BiosecurID the ideal benchmark for the study considered in this work.

Although, as highlighted above, the dynamic and static data of the database come from the exact same real signatures, some small variations may exist between both versions of one signature, mainly due to acquisition errors, e.g. (i) the user signed outside the predefined area, therefore, during the automatic segmentation process of the off-line sample, part of the signature is lost (i.e., strokes falling outside the paper signing grid); (ii) during the acquisition there was a misalignment between the tablet and the paper template placed on it, leading to a slight rotation difference between the static and dynamic versions of the signature; and (iii) also, in some cases, due to a short malfunction of the dynamic acquisition device, part of the on-line information is lost or incomplete.

As the database was acquired in five different venues, five different inking pens were used. Such ink variability among off-line samples could entail a performance deviation difficult to estimate and which falls out of the scope of the present work.

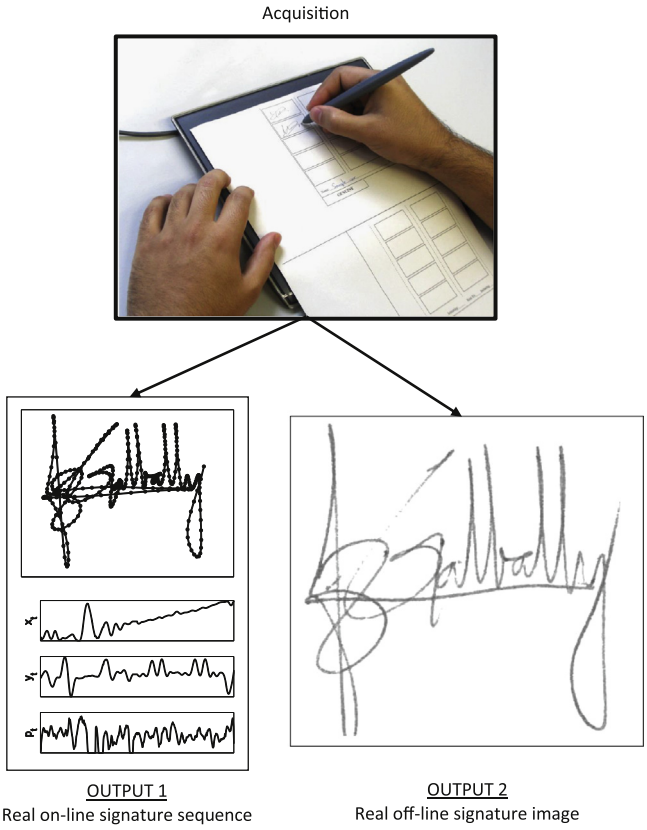

Fig. 2. Diagram of the BiosecurID DB acquisition process. Users signed on a paper template that limited the scaling and rotation variability, placed over a digitizing tablet. This way, the on-line and off-line versions of the same signature were acquired simultaneously.

To avoid this bias in the results, only the signature subcorpus captured at one of the venues, the Universidad Autonoma de Madrid, which is the largest within the database, will be considered in the work.

The BiosecurID-Signature UAM subcorpus comprises 132 users, with 16 genuine signatures (four per session) and 12 skilled forgeries (three per session) for every subject. Hence, the database contains the on-line and off-line data of $16 \times 132 = 2112$ genuine signatures and of $12 \times 132 = 1584$ skilled forgeries.

Genuine and skilled forgery real samples of the same user are shown in the first two rows of Fig. 3, where both the dynamic and static versions of the same signatures are depicted. In the second row, it may be noticed that the lowest part of the first off-line genuine signature image, as well as the top and bottom parts of the skilled forgery, is missing. As explained above, this is due to the automatic segmentation process that removes signature segments that fall outside the designated signing grid.

The *synthetic* off-line data used in the experiments was generated taking as input the on-line real signatures of the BiosecurID-Signature UAM database. That is, for each real on-line signature in the BiosecurID-Signature UAM DB (genuine or skilled forgery), its off-line synthetic version is produced following the methodology described in Section 3. Therefore, the synthetic off-line dataset presents exactly the same structure as the real version, that is 4 sessions, 132 users, 4 genuine signatures and 3 skilled forgeries per session and user.

Last row in Fig. 3 shows the synthetic static samples corresponding to the three real signatures depicted in the first two rows. As described in Section 3, synthetic signatures are defined by two different images: $I_{enhanced}$ (third row, top), which incorporates pressure and speed information from the real dynamic signature; and $I_{pen-ups}$ (third row, bottom), obtained from the signature trajectory during pen-ups. We can observe the high similarity existing between real (second row) and synthetic (third row) off-line samples.

Therefore, as presented in the current section, the experimental protocol described in Section 5 and depicted in Fig. 4, comprises three different versions of the exact same signatures: (i) real on-line version, (ii) real off-line version, and (iii) synthetic off-line version. The three complementary signature subsets are publicly available from the Biometric Recognition Group-ATVS webpage[1].

4.2. On-line and off-line signature recognition systems

In the experiments, two different on-line signature verification systems and one off-line signature system are used. All three systems have been selected from representative technologies available nowadays in the signature recognition state of the art.

The two dynamic signature recognition algorithms are based on totally different features and matchers. This way, as one of the main objectives set for the study, it will be possible to establish the impact that the fusion of a top-performing off-line signature verification system has on the overall accuracy of different on-line authentication strategies. These two systems are

- *On-line system A: function-based + DTW*. This function-based local approach uses a subset of nine time sequences selected using the Sequential Forward Floating Selection (SFFS) algorithm from the total set of functions defined in [22] (which includes, among others, the first and second order derivatives of x and y). The nine signals are directly matched using Dynamic Time Warping (DTW) [23]. The goal of DTW is to find an elastic match among samples of a pair of time sequences of different lengths that minimize a given distance measure. In this particular implementation, which is thoroughly described in [22], we use the Euclidean distance as the measure to be optimized and only three correspondences among samples of the compared sequences are allowed. The final score is computed as the average of the scores obtained between the test signature and the enrolled samples. This system ranked among the top three algorithms in all the tasks of the recent BioSecure Signature Evaluation Campaign BSEC-2009 [24].
- *On-line system B: feature-based + Mahalanobis distance*. This system models the signature as a holistic multidimensional vector composed of the best performing 40-feature subset extracted in [20] from the total set of 100 global features described in [19]. In the present study, we used this 40-feature representation of the signatures normalizing each of them to the range [0,1] using tanh-estimators [25]. Finally, the similarity scores are computed using the Mahalanobis distance between the input vector and a statistical model of the attacked client estimated using a number of training signatures.

The offline signature verifier used in the experimental protocol is based on texture descriptors and a Support Vector Machine Classifier (SVM), as described below:

- *Off-line system C: LBP + SVM*. The system used for the evaluation of the real and synthetic signatures is a fusion of two LS-SVM classifiers [26], trained to work with Local Binary Patterns (LBP) and Local Directional Patterns (LDP), respectively. Signature images are divided into twelve overlapping blocks and the corresponding features are extracted. Dimensionality is then

[1] http://atvs.ii.uam.es/index

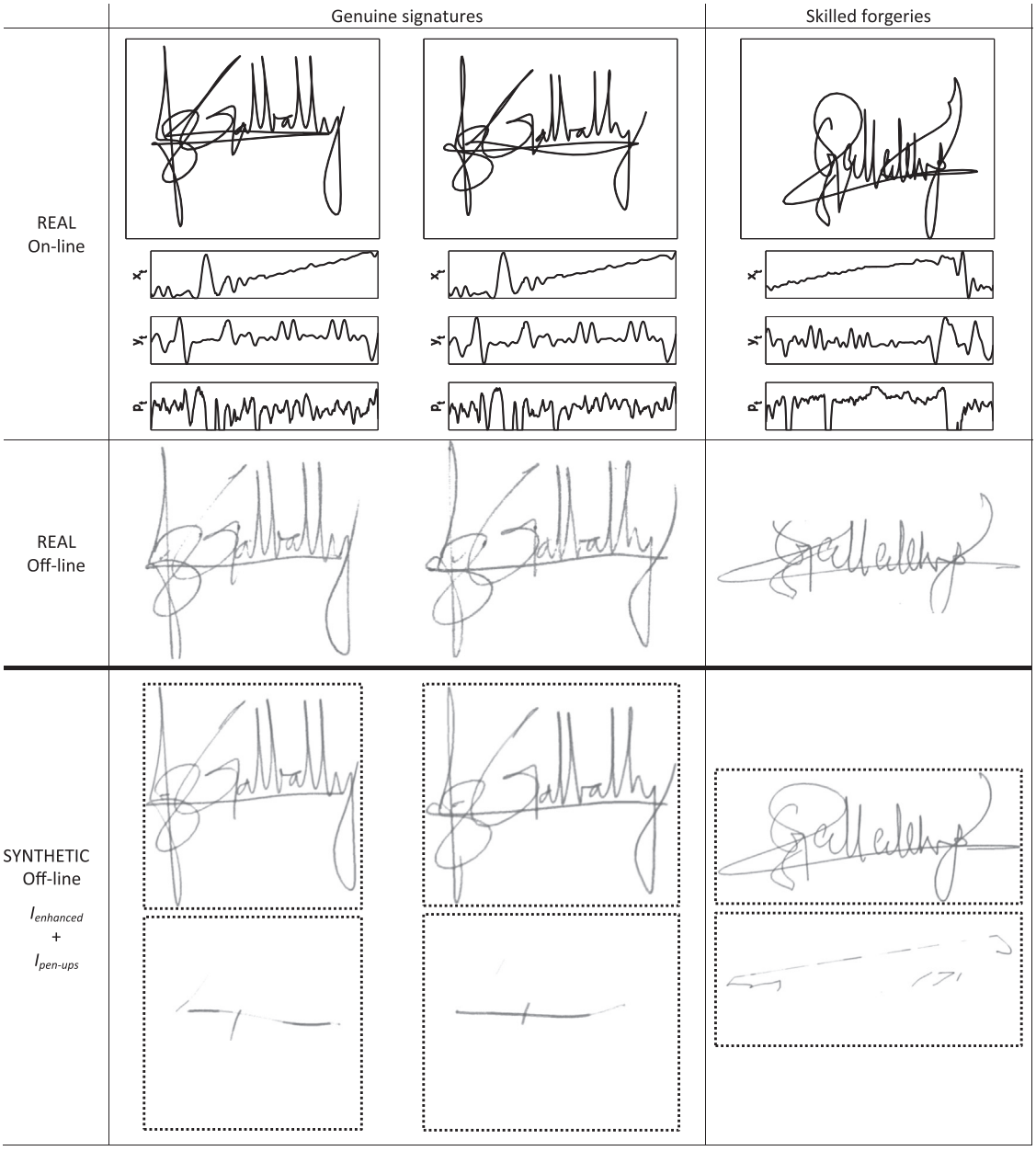

Fig. 3. Real on-line, real off-line and synthetic off-line versions of typical signature examples that can be found in the BiosecurID-Signature UAM database used in the experiments. Two genuine samples (first two columns) and a skilled forgery (last column) of the same user are shown. On-line samples are depicted with their corresponding time functions (x and y trajectories and pressure function p). Synthetic samples were generated following the method described in Section 3. Each synthetic signature is defined by two images: $I_{enhanced}$ (third row, top) and $I_{pen-ups}$ (third row, bottom). The whole database (real on-line, real off-line and synthetic off-line) is publicly available from the Biometric Recognition Group-ATVS webpage.

reduced using the Discrete Cosine Transform, and the final score is computed as the sum of the two partial scores coming from each of the classifiers. This system would have ranked second with an overall error (OE) of 11.4% at the very challenging off-line signature verification competition 4NSig-Comp2010 [27] (the winning system had a 8.9% OE, while all other algorithms presented an OE over 16%).

In the present work, the previous LS-SVM system is adapted to work with the dynamically enhanced synthetic off-line signatures generated according to the method described in Section 3. As shown in Fig. 1, each synthetic sample is represented by an enhanced image, $I_{enhanced}$, and an image comprising only the pen-up information $I_{pen-ups}$. Both images are parameterized separately and their LBP and LDP features concatenated to feed each of the two LS-SVM classifiers.

5. Experimental protocol

The experimental protocol has been designed to comply with the objectives set in the introduction of the work. For this purpose, it uses the databases and systems described in Section 4 in order to carry out three different experiments as depicted in Fig. 4. Each of the three evaluation experiments has been defined to fulfill some specific goals:

- *Experiment* 1: *monomodal*. The main objective of this experiment is to assess the individual performance of the three on-line and off-line verification systems described in Section 4.2. The off-line recognition algorithm is evaluated both on the real and synthetic static data. This way, a total of four performance results are obtained for this experiment (in blue in Fig. 4),

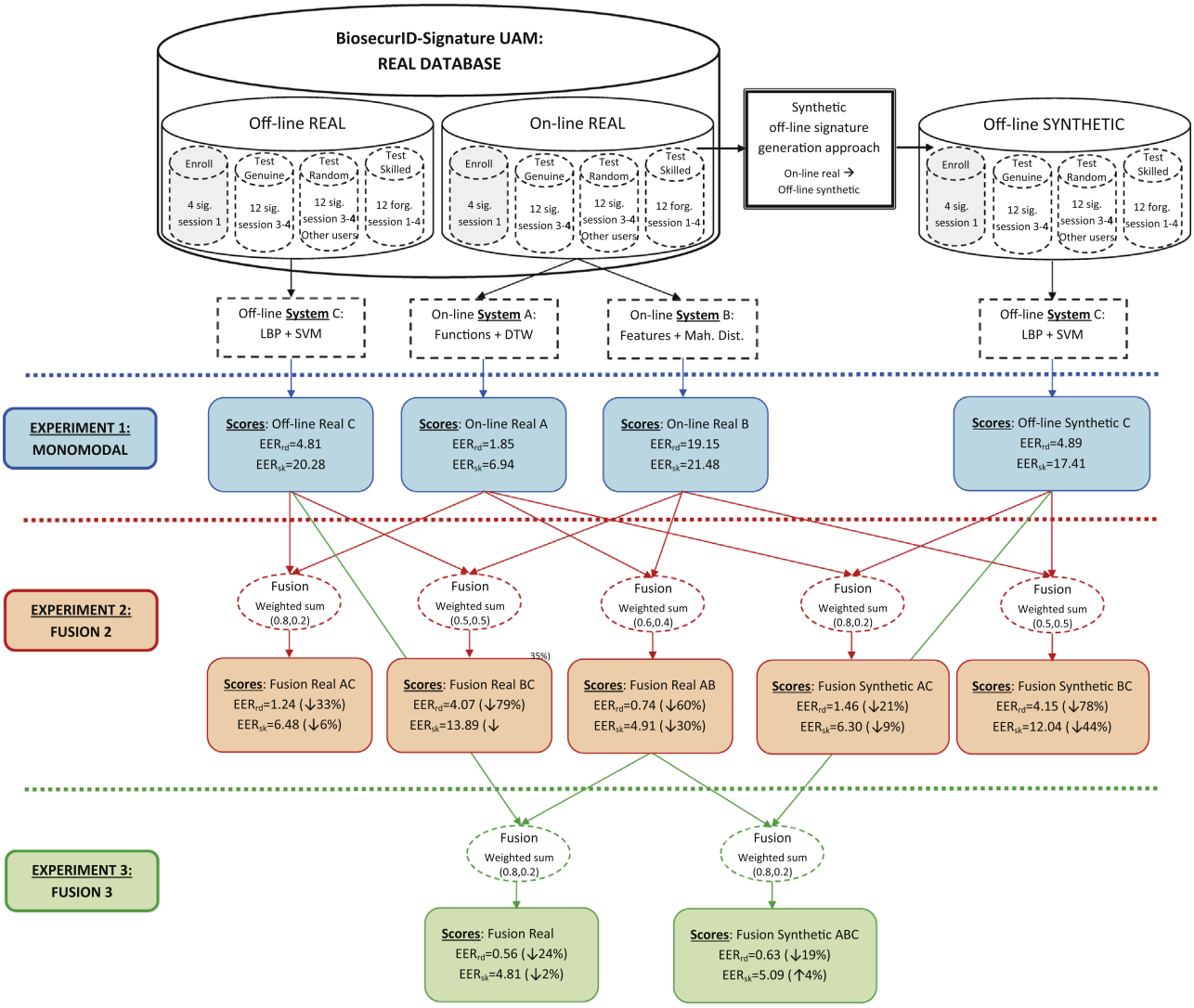

Fig. 4. Diagram of the experimental protocol followed in the work. The protocol together with the objectives of each of the three experiments, highlighted in the figure, is described in Section 5. Further details on the databases and the on-line and off-line recognition systems may be found, respectively, in Section 4.1 and 4.2. For each experiment the EER is given in percentage for the random forgeries EER_{rd} and the skilled forgeries EER_{sk} scenarios. In the fusion experiments, the percentage to the right of each EER refers to the performance improvement with respect to the best of the individual on-line verification systems fused. The higher weight of the fusion rules always corresponds to the best of the two combined systems. All results and figures are further explained in Section 6. (For interpretation of the references to colour in this figure, the reader is referred to the web version of this paper).

named according to the type of data used (on-line real, off-line real or off-line synthetic) and the recognition system evaluated (A, B or C): on-line real A, on-line real B, off-line real C and off-line synthetic C.

For each of the four performance results mentioned above, three sets of scores are computed: genuine, impostor random and impostor skilled. As depicted in Fig. 4, all users are enrolled to the system using their 4 first session signatures. Genuine scores are computed comparing the enrolled model to the 12 remaining genuine samples from the other three sessions, leading to $132 \times 12 = 1584$ genuine scores. Impostor scores for the random scenario are computed comparing the enrolled models to the 12 samples of sessions 1–3 from the remaining users, which makes a total of $132 \times 131 \times 12 = 207,504$ random impostor scores. While, finally, impostor scores for the skilled scenario are obtained matching the enrolled model to all 12 skilled forgeries available for that user, producing $132 \times 12 = 1584$ skilled impostor scores.

For the case of the genuine and skilled impostor scores, the protocol described above is repeated four times, using each time as enrollment samples the four genuine signatures corresponding to each of the four sessions. This way, the final number of scores is $4 \times 1584 = 6336$ genuine scores, $1 \times 207,504 = 207,504$ random impostor scores and $4 \times 1584 = 6336$ skilled impostor scores. These sizes of the three score sets are maintained in the following two experiments (i.e., fusion 2 and fusion 3).

This experiment will allow reaching the following objectives: (i) fairly compare the performance of on-line and off-line verification systems under the exact same benchmark (database and protocol) for the random and skilled scenarios; (ii) compare the performance of the off-line verification system on real and synthetic data as a way to validate the synthetic generation approach proposed; and (iii) set the baseline results to be compared with experiments 2 and 3.

- *Experiment* 2: *fusion* 2. In this case, as shown in red in Fig. 4, results from experiment 1 are combined on a two by two basis. The new scores are named according to the two fused results. The fusion rule selected is the largely used weighted sum [28,29], which is applied after normalizing the scores to the

[0,1] range. Weight selection has been based on some preliminary development experiments, finally setting them to the values shown in Fig. 4 (the higher weight always corresponds to the best of the two fused systems).

The goals targeted with this experiment are (i) evaluate the complementarity of state of the art on-line and off-line verification approaches by assessing the performance improvement that can be achieved through their fusion (Fusion Real AC, BC); (ii) evaluate whether the performance reached combining on-line real data with off-line real data is similar to that obtained when static synthetic data is used (Fusion Real AC, BC vs Fusion Synthetic AC, BC); (iii) compare the fusion of on-line and off-line systems to the case of combining two different on-line recognition algorithms (Fusion Real AC, BC vs Fusion Real AB).

- *Experiment* 3: *fusion* 3. This scenario is similar to the one studied in experiment 2. However, in this test all three systems considered in the experimental protocol are combined using only real data in one case and synthetic off-line samples in the other. Again, the fusion strategy and name convention followed to obtain the results are the same used in experiment 2 (in green in Fig. 4).

  Similar to experiment 2, these tests are thought to (i) determine if off-line verification can improve the performance of already fused on-line systems (Fusion Real ABC); and (ii) if real and synthetic static data also behave in a similar manner in this scenario (Fusion Real ABC vs Fusion Synthetic ABC).

6. Results

In this section the results from the three experiments described in the experimental protocol (Section 5) are presented. Figs. 5 and 6 are introduced to graphically illustrate two of the main objectives set for the work:

- Assess the efficiency of the synthetic off-line signature generation method presented in Section 3. For this purpose, in Fig. 5 we compare the performance of the off-line system C described in Section 5, working with real off-line signatures and with synthetic static samples. Both the random forgeries (left) and the skilled forgeries (right) scenarios are shown. The results are depicted in terms of the Detection Error Trade-off (DET) curves which represent in one plot the two types of errors that may occur in biometric verification systems: the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). As a meaningful performance metric, the Equal Error Rate (i.e., EER, operating point where both the FAR and FRR are equal) also appears in each of the DET plots.
- Determine whether on-line signature recognition can be improved through the use of synthetic off-line data. For this purpose, the performance of the on-line systems considered in the experiments (i.e., systems A, B and AB) is directly compared to the performance of their fusion with synthetic static signatures (i.e., systems AC, BC and ABC synthetic). In order to establish such comparison in an easy manner and to be able to extract meaningful conclusions, results for the random and skilled scenarios are depicted in Fig. 6 using as before DET curves.

All the EERs corresponding to the DET plots shown in Figs. 5 and 6 are summarized in Table 1 together with their 95% confidence intervals.

For a detailed description of the experiment and its objectives e see Section 5. A visual representation of the experiments can be found in Fig. 4. Also in Fig. 4, the EER for all the tests may be consulted as a tool for quick reference and comparison among tests. The EER appears in percentage for the random forgeries EER_{rd} and the skilled forgeries EER_{sk} scenarios. In the fusion experiments in Fig. 4, the percentage to the right of each EER refers to the performance improvement with respect to the best of the individual on-line verification systems fused.

6.1. Experiment 1 – monomodal: results

For this experiment we will focus on the analysis of (i) the DET curves shown in Fig. 5 corresponding to the evaluation of the off-line signature verification system C; and (ii) the EERs shown in Table 1 corresponding to the individual on-line systems A and B and off-line system C. Several interesting conclusions may be

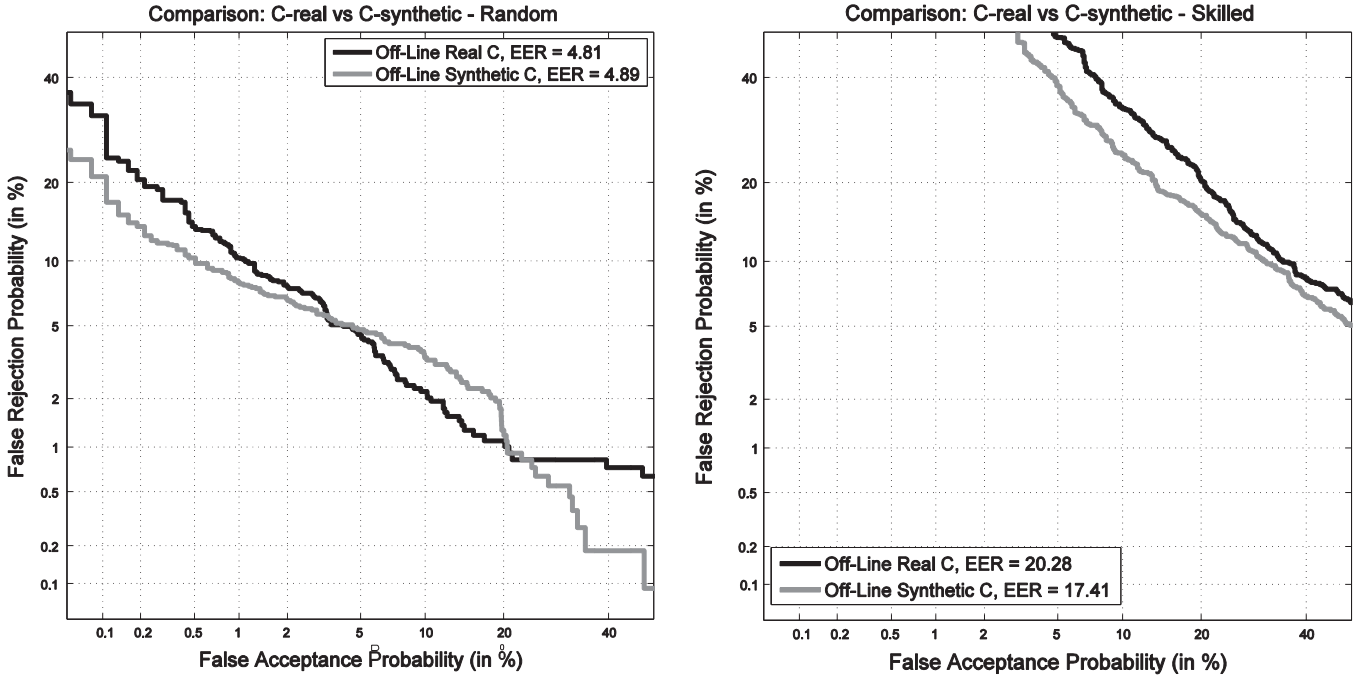

Fig. 5. Comparative DET curves for the off-line system C working with real off-line signatures and synthetic off-line signatures. Both the random (left column) and skilled (right column) impostors scenarios are shown. Results are interpreted and conclusions extracted in Section 6.

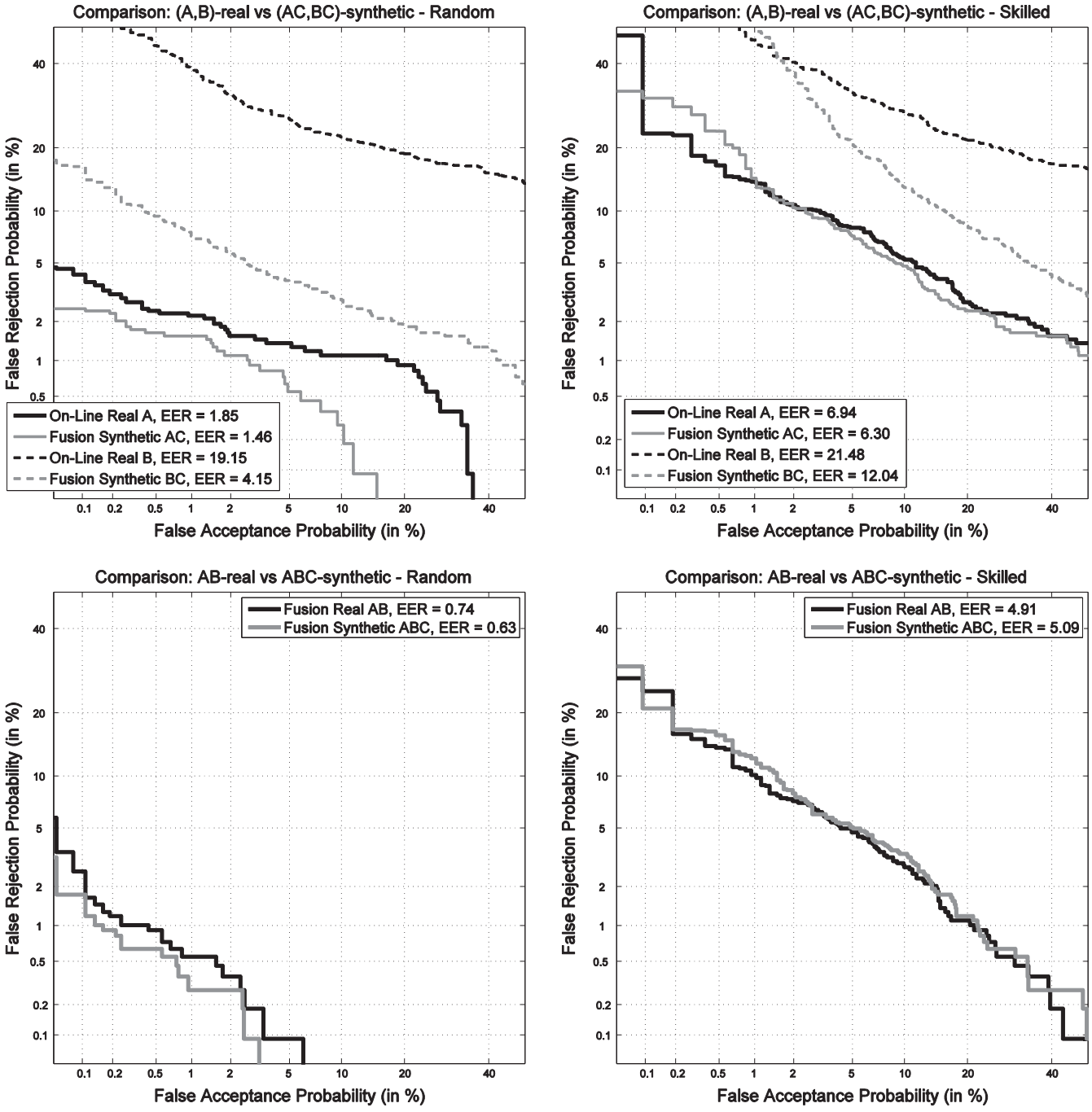

Fig. 6. Comparative DET curves for the on-line systems considered in the experiments (i.e., A, B and AB) and their fusion with synthetic off-line data (i.e., AC, BC and ABC). Both the random (left column) and skilled (right column) impostors scenarios are shown. Results are interpreted and conclusions extracted in Section 6.

Table 1
Comparative table of the EERs for the DETs shown in Figs. 5 and 6. Both the random and skilled forgeries scenarios are considered. The 95% confidence intervals of the EERs are shown in parenthesis.

Scenario	**Comparison: EER in % (± 95% confidence interval in %)**							
	C-real	C-synth.	A	AC	B	BC	AB	ABC
Random	4.81 (± 0.53)	4.89 (± 0.53)	1.85 (± 1.33)	1.46 (± 0.3)	19.15 (± 0.97)	4.15 (± 0.49)	0.74 (± 0.21)	0.63 (± 0.19)
Skilled	20.26 (± 0.99)	17.41 (± 0.93)	6.94 (± 0.63)	6.30 (± 0.6)	21.48 (± 1.01)	12.04 (± 0.8)	4.91 (± 0.53)	5.09 (± 0.54)

extracted from these results when they are compared on a two by two basis:

- *"Off-line Real C" vs "On-line Real A"*: These results confirm on a public, replicable and objective benchmark, what was already pointed out in several previous works [8,18]: dynamic signature contains more information than its static version and, therefore, can lead to lower error rates when two highly competitive on-line and off-line recognition algorithms (systems A and C) are compared.
- *"Off-line Real C" vs "On-line Real B" random scenario*: The previous observation does not hold in the random impostor scenario if the selected on-line recognition system is medium- or low-performing (system B). That is on-line verification algorithms have the potential to, but do not *necessarily* outperform static-based ones. This depends on the algorithms compared.
- *"Off-line Real C" vs "On-line Real B" skilled scenario*: In the case of skilled forgeries, even top-ranked off-line algorithms (system C) fail to achieve lower error rates than medium- or low-performing on-line systems (system B). Such an observation reinforces the largely extended belief that forgers tend to imitate the shape and geometry of the signatures in order to produce a similar "drawing", paying less attention to how that drawing was produced (i.e., the dynamics of the signature). Furthermore, in general it is easier to obtain the geometric information of a signature (i.e., off-line version) than its dynamic features (i.e., on-line version). For the latter case, the attacker would need to be present at the moment of the signing and, even in that case, he would only be able to witness the process once. Therefore, for the skilled forgeries scenario, on-line signature recognition appears to be, almost independent of the system considered, a more reliable technology than static-based recognition.
- *"Off-line Real C" vs "Off-line Synthetic C"*: The DET curves corresponding to these two experiments are almost superimposed (see Fig. 5), which means that the tested off-line recognition system (system C) performs almost identically on real and synthetic static data for both impostor scenarios (random and skilled). Such a result implies that the proposed synthetic off-line signature generation approach produces synthetic data with very similar variability to real samples and, hence, can potentially be used to assess the performance of off-line recognition systems. It is also worth noting that the additional dynamic information integrated in the synthetic data (i.e., pen-ups and speed) results in a non-negligible performance improvement in the skilled impostors scenario where the EER decreases from 20.28% with real signatures to 17.41% with synthetic samples (a relative improvement of 17%). This sustains the hypothesis that forgers try to imitate the signature shape, while neglecting the dynamics or the pen-up information for which, in general, they do not posses any information.

6.2. Experiment 2 – fusion 2: results

In this case we will focus on the analysis of the DET curves shown in the first row of Fig. 6 where the individual on-line systems (real A and real B) are compared to their fusion with synthetic off-line data (synthetic AC and synthetic BC). Several observations can be made in view of these results:

- *"On-line Real X" vs "Fusion Synthetic XC" random*: Here *X*C is used as a generic name to refer to both on-line systems A and B. These results show that synthetic off-line signature data (fused systems AC and BC) can significantly improve the performance of on-line signature verification algorithms (systems A and B), in this case the increase is as high as 33% and 79% in terms of the EER. This observation should be highlighted as one of the most important findings of the present article: synthetic static signature and real dynamic information present a large degree of complementarity that can be exploited to improve the accuracy of even top-performing dynamic-based algorithms (e.g., system A).
- *"On-line Real X" vs "Fusion Synthetic XC" skilled*: As before, *X*C is used as a generic name to refer to both on-line systems A and B. The previous conclusion cannot be generalized to the skilled impostor scenario. In this case, synthetic static data only contributes to increase the verification accuracy of medium- or low-performing on-line algorithms such as system B, which presents a relative EER improvement of 35%. However, the addition of synthetic off-line information has barely any effect on dynamic systems with already very low error rates such as system A (relative improvement of 6%). This result supports the hypothesis that almost all the information used to detect skilled forgeries is contained within dynamic data.

6.3. Experiment 3 – fusion 3: results

The second row of Fig. 6 shows the DET curves corresponding to the fusion of the two on-line systems (real AB) and the fusion of all three verification algorithms systems (synthetic ABC). Two main conclusions can be drawn from these results:

- *"Fusion Real AB" vs "Fusion Synthetic ABC" random*: As was already shown in experiments 1 and 2 for unimodal on-line systems, the performance of multimodal dynamic verification (i.e., fusion of systems A and B) is also improved both by real and synthetic off-line data under the random impostor scenario (with relative improvements in terms of the EER of 24% and 28%, respectively). This confirms the complementarity of the information comprised in static and dynamic data noted in previous experiments. It also reinforces one of the main contributions of the present work already pointed out in experiment 2: synthetic off-line signatures can be used to improve the performance of on-line recognition systems (even if these are the result of the fusion AB of two individual systems A and B).
- *"Fusion Real AB" vs "Fusion Synthetic ABC" skilled*: Similar to what was already observed in experiment 2, in the case of skilled forgeries there is technically no performance gain due to the large performance difference between the on-line algorithm (fusion of systems A and B) and the static-based algorithm (system C). In this scenario, the information added by static data is not enough to enhance the overall verification accuracy.

6.4. Results summary

As already mentioned, all the results presented in Sections 6.1–6.3 are graphically summarized in terms of the EER and its relative improvement in Fig. 4. The observations and conclusions extracted from these results in the previous sections may be summarized as follows:

- As already mentioned in the discussion of the individual experiments, probably the most important contribution of the article is that *synthetically generated off-line data can be used to significantly and consistently improve the performance of dynamic signature recognition systems in the random scenario*, independent of whether these are individual systems (e.g., A or B) or a fusion of several on-line matchers (e.g., AB). This conclusion is drawn from the comparison of results (see Fig. 6 and Table 1):

system A vs AC-synthetic, system B vs BC-synthetic, system AB vs ABC-synthetic. The average relative improvement obtained in this scenario is of 40%, with an increase in the accuracy as high as 20% for even top performing algorithms.

- The same comparative results show that (see Fig. 6 and Table 1) *In the skilled forgery scenario the previous observation only holds for low- to medium-performing on-line signature recognition systems* (system B vs BC-synthetic). In the case of competitive on-line verification algorithms their performance is maintained (it does not decrease).
- Real off-line data and synthetic off-line data, generated from dynamic information following the approach proposed in Section 3, behave almost identically in the random impostor scenario (i.e., see the comparison C-real vs C-synthetic in Fig. 5 and Table 1).
- Regarding the same comparison (i.e., C-real vs C-synthetic shown in Fig. 5 and Table 1), in the case of skilled forgeries the synthetic samples present a higher discriminative power (relative improvement of 17%), probably due to the addition of motion information (i.e., speed and pen-up trajectories) in the generation process.
- On-line data contain more information than off-line data and therefore can potentially lead to lower error rates (i.e., system A vs C). This observation is stronger for the skilled impostor scenario where it holds even for low-performing on-line systems (i.e., system B vs C). This conclusion reinforces the largely extended belief that forgers tend to imitate the shape and geometry of the signatures in order to produce a similar "drawing", paying less attention to how that drawing was produced (i.e., the dynamics of the signature). Therefore, the on-line modality has a much larger discriminative potential against skilled impostors.

In view of the previous summary, we propose a novel architecture for on-line verification, which exploits the complementarity of dynamic and static signature recognition through the generation of synthetic off-line data. The new method tries to solve the traditional on-line vs off-line dichotomy, taking the best from both modalities. Like any other on-line verification system, the proposed approach receives only two inputs (see the diagram in Fig. 7): the real enrolled on-line model and the real dynamic test signature (which can be a genuine sample, random impostor or skilled impostor). These two inputs are matched using any generic on-line signature verification approach (either an individual system or fusion of different matchers) to produce a single on-line score s_{on}. Simultaneously, the two on-line inputs are transformed into synthetic static samples which are compared using any off-line verification system, generating this way a single off-line score s_{off}. Finally, the two scores (on-line and off-line) are combined to produce one single output s.

The methodology is general, since it can integrate (i) any on-line verification system either unimodal (such as systems A and B considered in the present work) or multimodal, as combination of several algorithms (such as the fusion AB used in the experiments); (ii) any off-line verification system (such as system C considered in the present work); (iii) any fusion strategy to combine the on-line (s_{on}) and off-line (s_{off}) matching scores.

Another added value of this architecture is its high practical potential for real world applications. The proposed approach does not need any further requirements with respect to currently deployed on-line verification systems: from two input dynamic signatures one similarity score is generated. The performance improvement is obtained at the expense of a small increase in the system response time due to the computational cost derived from (1) the generation of the off-line synthetic samples; (2) the matching of the off-line synthetic samples. In the particular case of the experiments presented in this paper, carried out on MATLAB 2012a running on a standard core i6 PC using windows 7, such extra computational cost was on average around 0.3 s, for every matching transaction. Such an increase in the system's throughput would be acceptable for most real operational contexts.

7. Conclusions

When dealing with an on-line verification problem, it should be assumed that off-line data is not available. However, in the present work, a method to generate synthetic static samples from on-line signatures has been proposed. It has been experimentally shown that the behaviour of such synthetic samples is very similar to their real off-line versions, and that they can complement on-line information.

This way, one of the main contributions of the work is the use of the novel generation method to fuse both types of data, real on-line and synthetic off-line, in order to improve the performance of on-line verification algorithms. The level of improvement achieved through this fusion depends on the impostor scenario considered:

- *Random impostors*: As already mentioned in the introduction, this represents a very relevant scenario, as the decision threshold of most applications is fixed according to the error rates obtained in this operational framework. As such, it defines in many cases the baseline performance of the system. The very significant performance boost obtained in this case through the fusion of the synthetic off-line data with the three on-line systems tested is, on average, of 40%.
- *Skilled impostors*: This is the most relevant scenario in forensic-related applications. In this case, the accuracy of on-line systems is only improved through the fusion with synthetic static data if the original algorithm presented a low-performance. For top-ranked on-line systems the performance is, in the worst case, preserved.

Another significant value of the work is the synthetic off-line signatures generation method proposed. The synthetic static samples are "dynamically enhanced", embedding part of the time-related information of the original on-line signatures (e.g., speed and pen-up trajectories). This way, their discriminative power in the skilled impostors scenario is increased with respect to regular real static signatures where only the image is available.

In summary, three main contributions may be highlighted from the present research work with respect to the current state of the art in signature biometrics: (i) a new method for the generation of "dynamically enhanced" synthetic off-line signatures starting from real on-line data has been proposed; (ii) different findings regarding the discriminative capabilities and the complementarity of off-line and on-line signature in the random and skilled forgeries scenarios have been extracted, using a public benchmark which contains the dynamic and static versions of the same signatures; and (iii) a new on-line signature recognition architecture based on the combination of real dynamic data and synthetic static data has been proposed. The architecture has been validated on the same benchmark as top-ranked traditional algorithms, showing that, depending on the scenario and the systems considered, a significant performance improvement can be achieved.

This research reinforces the findings of previous works showing that, even though on-line signature has a higher potential for recognition tasks, it does not comprise all the information present in the signature trait. This way, off-line data can be a very valuable asset to significantly increase the overall performance of this biometric trait. Furthermore, the generation of synthetic static data can become a realistic alternative to close the dichotomy between on-line and off-line signature and promote research

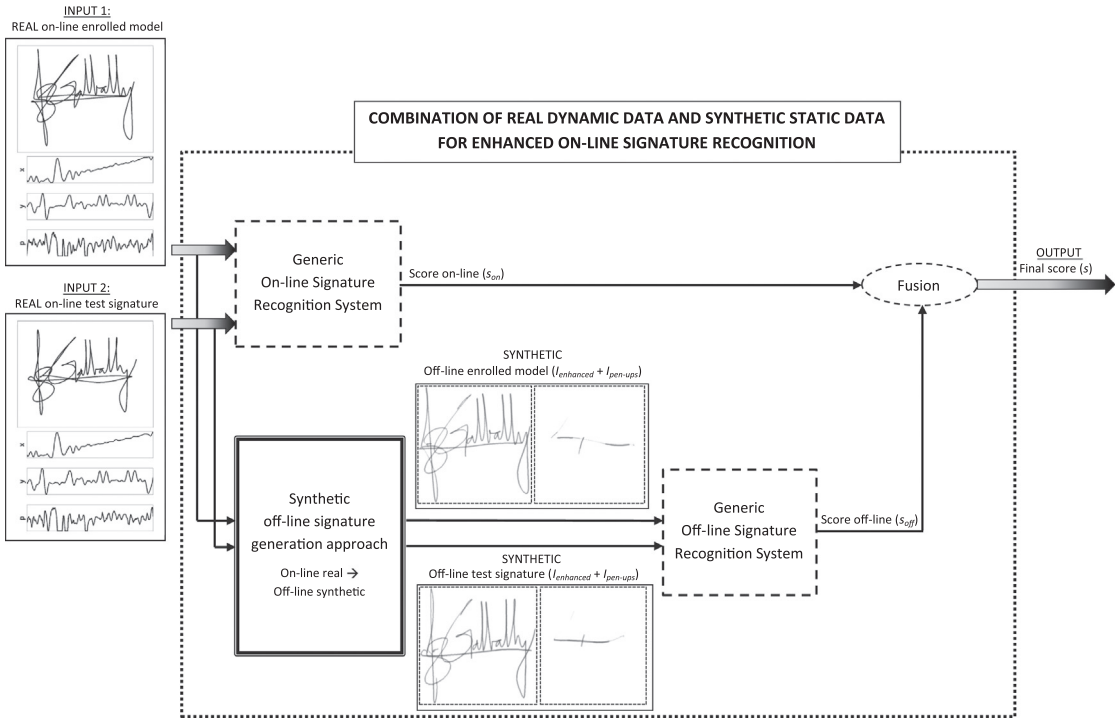

Fig. 7. Diagram of the novel on-line signature recognition architecture proposed in the present work. The use of synthetic off-line data to complement the dynamic inputs is supported by the results presented in Section 6 and summarized in Fig. 4.

towards a unified signature biometric that benefits from both modalities in order to reach the degree of deployment that was foreseen for this technology some years ago.

Conflict of interest

None declared.

Acknowledgements

M.D.-C. is supported by a Ph.D. fellowship from the ULPGC and M.G.-B. is supported by a FPU fellowship from the Spanish MECD (FPU2012/02134). A.M. is supported by a post-doctoral Juan de la Cierva contract by the Spanish MECD (JCI-2012-12357). This work has been partially supported by projects: BioSint (TEC2012-38630) and, Bio-Shield (TEC2012-34881) from Spanish MINECO, BEAT (FP7-SEC-284989) from EU, *CECABANK* and *Cátedra UAM-Telefónica*.

References

[1] R. Plamondon, G. Lorette, Automatic signature verification and writer identification—the state of the art, Pattern Recognit. 22 (1989) 107–131.
[2] F. Leclerc, R. Plamondon, Automatic signature verification: the state of the art, 1989–1993, Int. J. Pattern Recognit. Artif. Intell. 8 (1993) 643–660.
[3] M. Fairhurst, Signature verification revisited: promoting practical exploitation of biometric technology, Electron. Commun. Eng. J. 9 (1997) 273–280.
[4] R. Plamondon, S.N. Srihari, On-line and off-line handwriting recognition: a comprehensive survey, IEEE. Trans. Pattern Anal. Mach. Intell. 22 (2000) 63–84.
[5] D. Impedovo, G. Pirlo, Automatic signature verification: the state of the art, IEEE Trans. Syst. Man Cybern. Part C: Appl. Rev. 38 (5) (2008) 609–635.
[6] J. Fierrez, J. Ortega-Garcia, On-line signature verification, in: Handbook of Biometrics, Springer US, New York, 2008, pp. 189–209.
[7] J. Galbally, M. Martinez-Diaz, J. Fierrez, Aging in biometrics: an experimental analysis on on-line signature, PLoS One 8 (2013) e69897.
[8] F. Alonso-Fernandez, J. Fierrez-Aguilar, M. Martinez-Diaz, J. Ortega-Garcia, Fusion of static image and dynamic information for signature verification, in: Proceedings of IEEE International Conference on Image Processing (ICIP), 2009, pp. 2725–2728.
[9] J. Galbally, R. Plamondon, J. Fierrez, J. Ortega-Garcia, Synthetic on-line signature generation. Part I: Methodology and algorithms, Pattern Recognit. 45 (2012) 2610–2621.
[10] M.A. Ferrer, M. Diaz-Cabrera, A. Morales, Synthetic off-line signature image generation, in: Proceedings of IAPR International Conference on Biometrics (ICB), 2013.
[11] M.A. Ferrer, J. Galbally, M. Diaz-Cabrera, A. Morales, M. Gomez-Barrero, Realistic synthetic off-line signature generation based on synthetic on-line data, in: Proceedings of IEEE International Carnahan Conference on Security Technology (ICCST), 2013, pp. 116–121.
[12] J. Galbally, J. Fierrez, J. Ortega-Garcia, R. Plamondon, Synthetic on-line signature generation. Part II: Experimental validation, Pattern Recognit. 45 (2012) 2622–2632.
[13] M.A. Ferrer, M. Diaz-Cabrera, A. Morales, Static signature synthesis: A neuromotor inspired approach for biometrics, IEEE Trans. Pattern Anal. Mach. Intell., 37 (2015) 667–680.
[14] A. Zimmer, L.L. Ling, A hybrid on/off line handwritten signature verification system, in: Proceedings of IEEE International Conference on Document Analysis and Recognition (ICDAR), 2003, pp. 424–428.
[15] Y. Qiao, J. Liu, X. Tang, Offline signature verification using online handwriting registration, in: Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition (CVPR), 2007.
[16] M. Vatsa, R. Singh, P. Mitra, A. Noore, Signature verification using static and dynamic features, in: Proceedings of International Conference on Neural Information Processing (ICONIP), LNCS-3316, Springer, 2004, pp. 350–355.
[17] A. Al-Shoshan, Handwritten signature verification using image invariants and dynamic features, in: Proceedings of IEEE International Conference on Computer Graphics, Imaging and Visualisation (ICCGIV), 2006, pp. 173–176.
[18] G. Rigoll, A. Kosmala, A systematic comparison between on-line and off-line methods for signature verification with Hidden Markov Models, in: Proceedings of IEEE International Conference on Pattern Recognition (ICPR), 1998, pp. 1755–1757.
[19] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Penalba, J. Ortega-Garcia, D. Maltoni, An on-line signature verification system based on fusion of local and global information, in: Proceedings of IAPR International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), Lecture Notes in Computer Science, vol. 3546, Springer Berlin Heidelberg, Berlin, 2005, pp. 523–532.
[20] J. Galbally, J. Fierrez, J. Ortega-Garcia, Performance and robustness: a trade-off in dynamic signature verification, in: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2008, pp. 1697–1700.

[21] J. Fierrez, J. Galbally, et al., BiosecurID: a multimodal biometric database, Pattern Anal. Appl. 13 (2) (2010) 235–246.
[22] M. Martinez-Diaz, J. Fierrez, R.P. Krish, J. Galbally, Mobile signature verification: feature robustness and performance comparison, IET Biom. 3 (2014) 267–277.
[23] A. Kholmatov, B. Yanikoglu, Identity authentication using improved online signature verification method, Pattern Recognit. Lett. 26 (2005) 2400–2408.
[24] N. Houmani, A. Mayoue, et al., Biosecure signature evaluation campaign (BSEC2009): evaluating online signature algorithms depending on the quality of signatures, Pattern Recognit. 45 (2012) 993–1003.
[25] A.K. Jain, K. Nandakumar, A. Ross, Score normalization in multimodal biometric systems, Pattern Recognit. 38 (2005) 2270–2285.
[26] M. Ferrer, J. Vargas, A. Morales, A. Ordonez, Robustness of offline signature verification based on gray level features, IEEE Trans. Inf. Forensics Secur. 7 (3) (2012) 966–977.
[27] M. Blumenstein, M. Ferrer, J. Vargas, The 4NSigComp2010 off-line signature verification competition: Scenario 2, in: Proceedings of International Conference on Frontiers in Handwriting Recognition (ICFHR), 2010, pp. 721–726.
[28] J. Kittler, M. Hatef, R. Duin, J. Matas, On combining classifiers, IEEE. Trans. Pattern Anal. Mach. Intell. 20 (1998) 226–239.
[29] J. Fierrez-Aguilar, Adapted fusion schemes for multimodal biometric authentication (Ph.D. thesis), Universidad Politecnica de Madrid, 2006.

Javier Galbally received the M.Sc. in Electrical Engineering, in 2005, from Universidad de Cantabria, Spain, and the Ph.D. degree in Electrical Engineering, in 2009, from Universidad Autonoma de Madrid, Spain. He has carried out different research internships at worldwide leading groups in biometric recognition such as BioLab from Università di Bologna Italy, IDIAP Research Institute in Switzerland, the Scribens Laboratory at the École Polytechnique de Montréal in Canada, or the Integrated Pattern Recognition and Biometrics Laboratory (i-PRoBe) at the West Virginia University in the USA. His research interests are mainly focused on the security evaluation of biometric systems, but also include pattern and biometric recognition, synthetic generation of biometric traits and inverse biometrics. He is actively involved in European projects focused on biometrics and is the recipient of a number of distinctions, including IBM Best Student Paper Award at ICPR 2008, finalist of the EBF European Biometric Research Award 2009, and Best Ph.D. Thesis Award by the Universidad Autonoma de Madrid 2010.

Moises Diaz-Cabrera received two M.Tech degrees, in 2010: Industrial Engineering and Industrial Electronics and Automation Engineering and hold a M.Sc. in Intelligent Systems and Numerical Applications in Engineering (2011) as well as a M.Ed. in Secondary Education (2013), all from La Universidad de Las Palmas de Gran Canaria. He is currently pursuing the Ph.D. degree and his research areas include handwriting signature recognition, pattern recognition and computer vision. Also he has some experience in Intelligent Transportation Systems through collaborations with CICEI, at ULPGC, and VisLab, at University of Parma.

Miguel A. Ferrer received the M.Sc. degree in telecommunications, in 1988, and the Ph.D. degree, in 1994, both from the Universidad Politécnica de Madrid, Spain. He belongs to the Digital Signal Processing research group (GPDS) of the research institute for technological development and Communication Innovation (IDeTIC) at the University of Las Palmas de Gran Canaria in Spain where he is an Associate Professor since 1990. His research interests lie in the fields of computer vision, pattern recognition, biometrics, databases and audio quality evaluation.

Marta Gomez-Barrero received her M.Sc. in Computer Science and her M.Sc. in Mathematics, in 2011, from Universidad Autonoma de Madrid, Spain. She is currently pursuing her Ph.D. degree with the Biometric Recognition Group – ATVS at Universidad Autonoma de Madrid, where she is working as an assistant researcher since 2010. In 2012 she was awarded with a FPU research fellowship from Spanish MECD and in 2013 obtained the postgraduate Master in Computer Science and Electrical Engineering from UAM. Also in 2013 she was the recipient of the 2nd Archimedes Prize for young researches from Spanish MECD. She carried out a research internship at da/sec – Biometrics and Internet Security Research Group, at the Hochschule Darmstadt, Germany. Her current research focuses on vulnerabilities evaluations and template protection schemes for facial, iris- and signature-based recognition systems.

Aythami Morales Moreno received his M.Sc. degree in Telecommunication Engineering, in 2006, from Universidad de Las Palmas de Gran Canaria. He received his Ph.D degree from La Universidad de Las Palmas de Gran Canaria in 2011. He performs his research works in the Digital Signal Processing Group (GPDS) at Las Palmas de Gran Canaria University and he has performed research stays in the Biometric Research Laboratory at Michigan State University, the Biometric Research Center at Hong Kong Polytechnic University and the Biometric System Laboratory at University of Bologna. His research interests are focused on pattern recognition, computer vision, machine learning and biometrics signal processing. He is author of more than 30 scientific articles published in international journals and conferences. He has received awards from ULPGC, La Caja de Canarias, SPEGC, and COIT. He has participated in 7 National and European projects in collaboration with other universities and private entities.

Julian Fierrez received the M.Sc. and the Ph.D. degrees in telecommunications engineering from Universidad Politecnica de Madrid, Madrid, Spain, in 2001 and 2006, respectively. Since 2002 he has been affiliated with the Biometric Recognition Group (ATVS), first at Universidad Politecnica de Madrid, and since 2004 at Universidad Autonoma de Madrid, where he is currently an Associate Professor. From 2007 to 2009 he was a visiting researcher at Michigan State University in USA under a Marie Curie fellowship. His research interests and areas of expertise include signal and image processing, pattern recognition, and biometrics, with emphasis on signature and fingerprint verification, multi-biometrics, biometric databases, and system security. He has been and is actively involved in European projects focused on biometrics, and is the recipient of a number of distinctions for his research, including best Ph.D. in computer vision and pattern recognition in 2005–2007 by the IAPR Spanish liaison (AERFAI), Motorola best student paper at ICB 2006, EBF European Biometric Industry Award 2006, IBM best student paper at ICPR 2008, and EURASIP best Ph.D. award 2012.