Enhanced On-Line Signature Verification Based on Skilled Forgery Detection Using Sigma-LogNormal Features

Marta Gomez-Barrero, Javier Galbally, Julian Fierrez, Javier Ortega-Garcia
ATVS - Biometric Recognition Group, EPS, Universidad Autonoma de Madrid, Spain
{marta.barrero,javier.galbally,julian.fierrez,javier.ortega}@uam.es

Réjean Plamondon
Laboratoire Scribens, Département de Génie Électrique, École Polytechnique de Montreal, Canada
rejean.plamondon@polymtl.ca

Abstract

One of the biggest challenges in on-line signature verification is the detection of skilled forgeries. In this paper, we propose a novel scheme, based on the Kinematic Theory of rapid human movements and its associated Sigma LogNormal model, to improve the performance of on-line signature verification systems. The approach combines the high performance of DTW-based systems in verification tasks, with the high potential for skilled forgery detection of the Kinematic Theory of rapid human movements. Experiments were carried out on the publicly available BiosecurID multimodal database, comprising 400 subjects. Results show that the performance of the DTW-based system improves for both skilled and random forgeries.

1. Introduction

In the so-called Information Age in which identity authentication is of the utmost importance, biometrics have emerged as a reliable, fast and automatic identification technology. Among the different biometric traits (i.e., fingerprint, face, voice, iris, etc.), one of the most widely accepted is the signature: we are used to signing credit card invoices and contracts in an every day basis.

Even though the verification performance rates of signature based systems have reached significantly high standards, specially for random forgeries, skilled forgeries remain a big challenge for those systems. In the last decade, some research has been carried out on forgeries detection in off-line signatures. In order to address this problem, in [6, 7] an analysis of geometrical properties at sub-stroke level, such as the slope or the length of the sub-stroke, is proposed. Even though results are encouraging, experiments were carried out on small databases comprising 10 subjects. More recently, Madasu and Lovell proposed a forgery detection system based on fuzzy angle features [12]. A 100% accuracy is reported on a 40 subjects database.

In the field of on-line signature, the amount of research regarding skilled forgeries detection has been much more scarce. Hasaine and Al-Maadeed proposed a skilled forgeries and simulated signatures detector based on differences of on-line signals and their histograms [8]. They report Equal Error Rates (EERs) below 0.1% for the QU on-line signature DB (12 subjects) and for the ICDAR2009 signature verification competition dataset [3] (50 subjects).

In order to encourage further research efforts in the detection of skilled forgeries, several international signature verification competitions have recently included tasks on this topic, from 4NSigComp2010 [11] to SigWiComp2013 [13]. The comparison of the automatic results to forensic handwriting examiners opinions showed that those results were not far away from human expert decisions. However, the test sets considered comprised between 1 and 54 European writers and results worsened when the number of writers increased, thus raising the need for research on bigger and more statistically significant databases.

One common pitfall among those studies is that they focus on skilled forgeries detection but they do not apply that knowledge to improve the performance of signature verification systems, which is the main contribution of this work. Therefore, the objectives of this article are twofold, namely: propose i) a new method to detect on-line skilled forgeries based on the Sigma LogNormal model, and ii) a new general on-line verification scheme, which integrates the information given by a skilled forgery detector with the matching scores of a regular on-line verification system. The enhanced novel approach significantly improves the performance of top-ranked state-of-the-art matchers.

Even though most of the existing literature on skilled forgeries detection considers off-line signatures, according

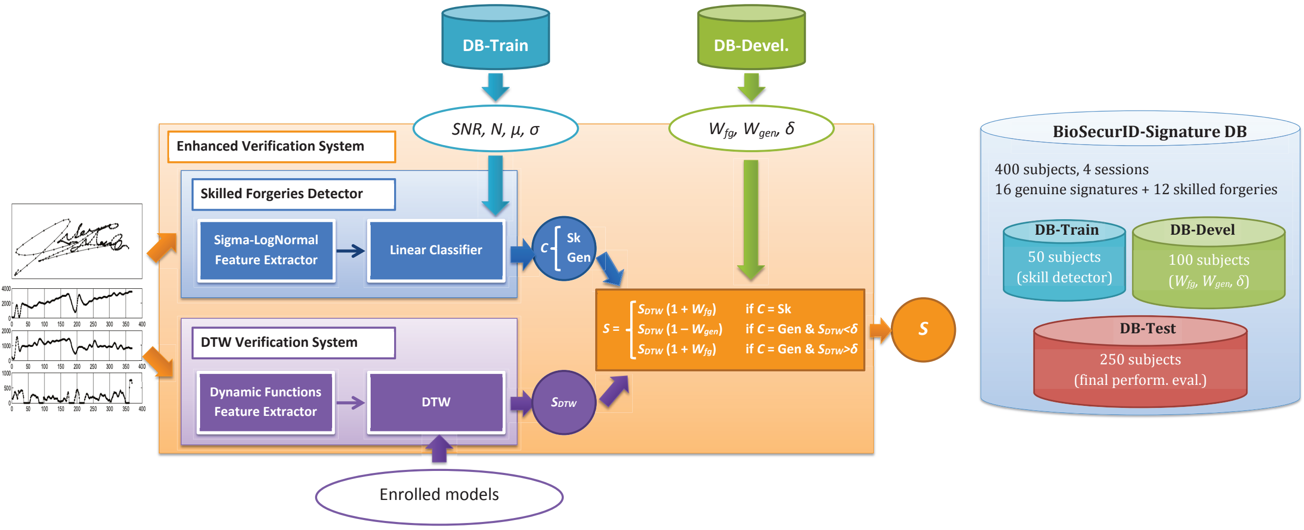
DB-Train
DB-Devel.
SNR, N, μ, σ
W_{fg}, W_{gen}, δ
Enhanced Verification System
Skilled Forgeries Detector
Sigma-LogNormal Feature Extractor
Linear Classifier
C
Sk
Gen
DTW Verification System
Dynamic Functions Feature Extractor
DTW
S_{DTW}
$S = \begin{cases} S_{DTW}(1+W_{fg}) & \text{if } C = \text{Sk} \\ S_{DTW}(1-W_{gen}) & \text{if } C = \text{Gen} \,\&\, S_{DTW}<\delta \\ S_{DTW}(1+W_{fg}) & \text{if } C = \text{Gen} \,\&\, S_{DTW}>\delta \end{cases}$
S
Enrolled models
BioSecurID-Signature DB
400 subjects, 4 sessions
16 genuine signatures + 12 skilled forgeries
DB-Train
50 subjects
(skill detector)
DB-Devel
100 subjects
(W_{fg}, W_{gen}, δ)
DB-Test
250 subjects
(final perform. eval.)

Figure 1. Diagram of the proposed enhanced on-line signature verification system and division of the database into training, development and test sets. For the training of the Linear Classifier, the train set in the database is used, while for the selection of the δ threshold and weights (W_{fg} and W_{gen}) the development set is utilized.

to document examiners, the key differences between genuine signatures and skilled forgeries include the speed, the pressure, the hesitation or the tremor [7, 12]. Therefore, the information provided by on-line signatures could be expected to be more reliable and accurate, as it is shown in the better results achieved on the on-line corpus in [10].

Regarding the different features that can be extracted from these on-line data, we have selected the approach based on the Kinematic Theory of rapid human movements, with its associated Sigma LogNormal representation of signatures [16]. The main advantage of this model is that it takes into account physical body features such as the neuromuscular system responsible for the production of a signature, and thus reflects some of the characteristics pointed out above, as the hesitation or the tremor.

Finally, it should be noted that most of the related works mentioned above report results on small and not always publicly available databases. In order to make our analysis reproducible and fairly comparable to future research, experiments are carried out on the multimodal BiosecurID database[1], whose on-line signature corpus comprises 11,200 signatures form 400 subjects (6,400 genuine signatures and 4,800 skilled forgeries).

The rest of the article is structured as follows: in Sect. 2, the proposed system is presented. The experimental protocol is described in Sect. 3 and results included in Sect. 4. Final conclusions are drawn in Sect. 5.

2. Proposed System

In order to improve the performance of on-line signature verification systems, we propose a scheme in which a new module, focused on the detection of skilled forgeries, is added to the original verification system (see Fig. 1). Depending on the output of this new module (i.e., genuine signature or skilled forgery), the score emitted by the initial verification system will be accordingly weighted, and the final decision will be based on this weighted score.

First of all, it should be noted that, whereas there are only two different sets of signatures (i.e., *genuine signatures* and *skilled forgeries*), signature verification systems deal with three sets of scores. In order to avoid confusion, the following terms will be used throughout the article:

- Signatures: given a user U_1,
  - *genuine signatures* are the genuine samples produced by the signer U_1,
  - *skilled forgeries* are forgeries of genuine signatures of U_1 produced by a different signer U_i, with $i \neq 1$.
- Scores: given a user U_1, and its corresponding user model M_1, three sets of scores are computed:
  - *genuine scores*, obtained comparing genuine signatures from U_1 to M_1,
  - *random impostor scores*, yielded by the comparisons between genuine signatures belonging to users U_i, with $i \neq 1$, and M_1,
  - *skilled impostor scores*, computed matching skilled forgeries of signatures of U_1 to M_1.

There are thus two sets of scores produced by genuine signatures: genuine scores and random impostor scores. A genuine acceptance threshold δ, computed over the original S_{DTW} scores, is introduced to separate them.

[1] See http://atvs.ii.uam.es/databases.jsp

Therefore, as it may be observed in Fig. 1, the following steps are performed to verify one signature:

- The skilled forgeries detector classifies the signature as either genuine (denoted as Gen) or skilled forgery (denoted as Sk). This detector, based on Linear Discriminant Analysis, LDA, takes four Sigma LogNormal parameters as input (N, SNR, μ and σ, see Sect. 2.1), and fits a multivariate Gaussian to each class. The final decision is a binary value: $C = \{\text{Gen, Sk}\}$.

- The baseline verification system, based on the very popular Dynamic Time Warping algorithm [15], outputs a dissimilarity score (i.e., lower scores correspond to more similar signatures, while higher scores correspond to different signatures) between the input signature and the enrolled user model, S_{DTW}.

- This score, S_{DTW}, emitted by the baseline verification system, will be weighted according to the decision of the skilled detector classifier, C, that is:

  $$S = \begin{cases} S_{DTW}(1 + W_{fg}) & \text{if } C\text{=Sk} \\ S_{DTW}(1 + W_{fg}) & \text{if } C\text{=Gen and } S_{DTW} > \delta \\ S_{DTW}(1 - W_{gen}) & \text{if } C\text{=Gen and } S_{DTW} < \delta \end{cases}$$

  where $W_{fg} \geq 0$ is the weight applied to scores that correspond to potential forgeries (skilled or random) while $W_{gen} \geq 0$ is applied to scores potentially produced by two signatures coming from the same user.

The rationale behind the proposed approach is to "support" or "strengthen" the score given by the DTW system (S_{DTW}) according to the decision of the skilled detection module (C) and the genuine acceptation threshold (δ). According to these inputs, if the detector believes that the score S_{DTW} corresponds to an impostor (either random, if C=Gen and $S_{DTW} > \delta$, or skilled, if C=Sk) the dissimilarity score will be enlarged ($S = S_{DTW}(1+W_{fg})$), that is, it will be biased toward a "more probable impostor" decision. The other way around, if the detector believes that it is a genuine score (if C=Gen and $S_{DTW} < \delta$) it will be made smaller ($S = S_{DTW}(1 - W_{gen})$), that is, biased toward a "more genuine" decision.

The final decision will thus be based on the weighted S dissimilarity score. If the baseline system outputs a similarity score (and not a distance metric or dissimilarity score as is this case), the signs corresponding to the weights W_{fg} and W_{gen}, and the comparison with δ, should be inverted.

2.1. The Sigma LogNormal Model

In the framework of the Kinematic theory for rapid human movements, the Sigma LogNormal model was developed as a new high level representation of on-line signatures [16], in which single strokes are considered as primitives from which complex patterns are built. Each primitive has a LogNormal velocity profile ($|v_i(t; P_i)|$) and a complex pattern is produced by summing up strokes, whose angular positions are determined by $\phi_i(t; P_i)$:

$$\begin{aligned} \phi_i(t; P_i) &= \theta_{di} + \frac{\theta_{fi} - \theta_{di}}{D_i} \int_0^t |v_i(\tau; P_i)| \mathrm{d}\tau \\ |v_i(t; P_i)| &= \frac{D_i}{\sigma\,(t - t_{0i})\,\sqrt{2\pi}} \exp\left(\frac{[\ln (t - t_{0i}) - \mu_i]^2}{-2\sigma_i^2} \right) \\ P_i &= (t_{0i}, D_i, \theta_{di}, \theta_{fi}, \mu_i, \sigma_i) \end{aligned}$$

Here P_i represents the parameters of the i-th stroke, where t_{0i} is the starting time, D_i its length, θ_{id} and θ_{fi} the starting and ending direction angles, μ_i the logtime delay and σ_i the logresponse time. These last two parameters characterize the LogNormal impulse response of the neuromuscular system. This model establishes the theoretical *ideal* representation of the signature, being the differences between this ideal model and the behaviour of the actual instance of a signature measured in terms of the Signal to Noise Ratio (SNR), defined over the velocity signals.

This theory is based on the human writing behaviour and it can be of great use in the very difficult task of skilled forgery detection. It has been shown that signing is a well-learnt movement very accurately represented by the Sigma LogNormal model. We may therefore assume that when an imitator produces a skilled forgery, he is not as trained as the genuine signer and the produced signatures will hence drift away from LogNormality. In particular, the Sigma LogNormal model is capable of detecting typical signing behaviours found in skilled forgeries and pointed out by calligraphic experts, such as: hesitation (which translates into a higher number of strokes or Sigma LogNormal curves in the velocity function N) and unnatural velocity profiles with very slow strokes.

In order to analyse the variations of the neuromuscular responses in the whole signature, not in each single stroke, we will focus on four parameters: N, SNR, and the averages across all the strokes of μ and σ.

2.2. On-Line Signature Verification with DTW

For the baseline signature verification system we chose the function-based local approach described in [15], which ranked among the top three algorithms at BSEC-2009 [9]. In this approach, 9 different time functions (selected using SFFS from a total of 34 features in [15]) are directly matched using an elastic technique, based on Dynamic Programming, known as Dynamic Time Warping (DTW) [15]. This algorithm offers a solution to the challenging problem of matching time sequences of variable lengths minimizing a pre-defined distance measure. In this particular implementation, the Euclidean distance is used and only three correspondences among samples are allowed.

Table 1. Performance of the skilled forgeries detector over the development and the test sets.

	GER	SER	HTER
Devel Set	13.56%	28.58%	21.07%
Test Set	14.53%	37.78%	26.15%

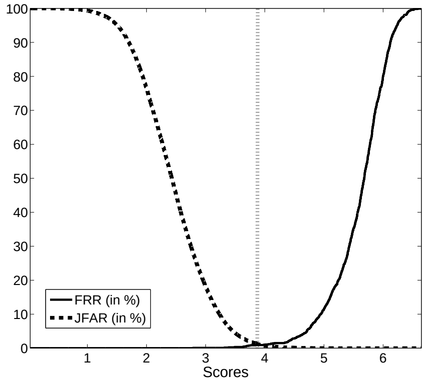

Figure 2. FRR and JFAR for the development set. The crossing point is marked by a vertical dashed line.

The final score output by the system (S_{DTW}) is computed as the average of the partial scores between the test sample and all the enrolled signatures of the user model.

3. Experimental Protocol

Experiments are carried out over the on-line signature corpus of the multimodal BiosecurID database [5]. It comprises 400 subjects with 16 original signatures and 12 skilled forgeries per user, created by the three following subjects. The database was captured in an office-like environment in four acquisition sessions, each separated two months. Users were asked to sign on a piece of paper placed on a Wacom Intuos 3 pen tablet, that captured the time signals of each signature at a 100 Hz sampling rate.

The database is divided into three independent sets, so that evaluation results are not biased (see Fig. 1 right): training set (first 50 subjects), development set (second 100 subjects) and test set (last 250 subjects). User models are enrolled with the 4 signatures belonging to session 1.

In order to evaluate the performance over the development or the test set, for each subject $i)$ genuine scores are computed comparing signatures of sessions 2, 3 and 4 (not used for enrolment) to the enrolled model of that same user, $ii)$ skilled impostor scores are obtained comparing all the skilled forgeries to their corresponding enrolled model, and $iii)$ random impostor scores are yielded matching the enrolled models to the first signature of the fourth session of the remaining users.

Finally, three steps have been followed to evaluate the performance of the proposed system, one on each of the sets in which the database is divided into:

- Step 1. Skilled forgery detector training (training set). Train the skilled forgeries detection module over the training set of the database.
- Step 2. Parameters optimization (development set). Define the genuine acceptation threshold δ over the raw S_{DTW} scores, in order to distinguish random impostor scores from genuine scores. Select best weights configuration (W_{fg}, W_{gen}) over the development set, in terms of the Equal Error Rate (EER) of the proposed system.
- Step 3: Performance evaluation (test set). Evaluate the configuration selected in the previous steps over the test set, in terms of the EER and the Detection Error Trade-off (DET) curves.

4. Results

The experiments follow the steps defined in Sect. 3 with a threefold objective:: $i)$ first estimate the potential of the Sigma LogNormal model to detect skilled forgeries, $ii)$ then find the best performing configuration of parameters (δ, W_{fg}, W_{gen}), and $iii)$ finally evaluate the proposed system performance over the test set. All sets of experiments are run over independent subsets of the database, so that the results are not biased.

4.1. Step 1: Skilled Forgery Detector Training

The training of the skilled forgery detector is carried out in two successive phases. First, the Sigma LogNormal parameters considered in the study [N, SNR, μ, σ] are extracted from all the signatures in the training set, that is: $50 \times 16 = 800$ genuine signatures and $50 \times 12 = 600$ skilled forgeries. Then, the feature vectors of genuine and skilled forgeries are used to train a linear classifier in order to distinguish between the two classes: genuine or skilled forgery.

The performance of the classifier is finally assessed on the development set over 1,600 genuine signatures and 1,200 skilled forgeries. The results are reported in Table 1 in terms of the Half Total Error Rate (HTER) defined as HTER=(GER+SER)/2, where the GER is the Genuine Error Rate (number of genuine signatures classified as forgeries) and the SER is the Skilled Error Rate (number of skilled forgeries classified as genuine). As it may be observed, the HTER achieved is 21% for the development set.

4.2. Step 2: Parameters Optimization

After training the skilled forgeries detector, the full system parameters (δ, W_{fg} and W_{gen}) are optimized in two steps over the development set (see Fig. 1 right). According to the experimental protocol defined in Sect. 3, a total number of $100 \times 12 = 1,200$ genuine, $100 \times 12 = 1,200$

Table 2. EERs, in %, on the development set for different values of the weights (W_{fg}, W_{gen}). The relative difference w.r.t. the baseline ($\mathrm{EER}_{\mathrm{sk}} = 3.58\%$ and $\mathrm{EER}_{\mathrm{rd}} = 0.93\%$) is shown in parentheses (in %), and in green (if EER improves) or red letter (if it worsens). The best configuration is highlighted in bold.

	Skilled Forgeries					Random Forgeries				
W_{gen} / W_{fg}	0	0.1	0.2	0.3	0.4	0	0.1	0.2	0.3	0.4
1.3	3.00 (↓ 16)	2.83 (↓ 21)	2.58 (↓ 28)	3.25 (↓ 9)	4.58 (↑ 28)	0.26 (↓ 72)	0.52 (↓ 45)	0.68 (↓ 27)	1.10 (↑ 18)	1.77 (↑ 90)
1.5	2.83 (↓ 21)	2.67 (↓ 26)	2.58 (↓ 28)	3.25 (↓ 9)	4.58 (↑ 28)	0.14 (↓ 85)	0.29 (↓ 68)	0.68 (↓ 27)	1.10 (↑ 18)	1.77 (↑ 90)
1.6	2.75 (↓ 23)	2.58 (↓ 28)	2.58 (↓ 28)	3.25 (↓ 9)	4.58 (↑ 28)	0.09 (↓ 90)	0.26 (↓ 72)	0.68 (↓ 27)	1.10 (↑ 18)	1.77 (↑ 90)
1.7	2.75 (↓ 23)	**2.50 (↓ 30)**	2.58 (↓ 28)	3.25 (↓ 9)	4.58 (↑ 28)	0.09 (↓ 90)	**0.21 (↓ 77)**	0.68 (↓ 27)	1.10 (↑ 18)	1.77 (↑ 90)
1.8	2.75 (↓ 23)	2.50 (↓ 30)	2.58 (↓ 28)	3.25 (↓ 9)	4.58 (↑ 28)	0.09 (↓ 90)	0.21 (↓ 77)	0.68 (↓ 27)	1.10 (↑ 18)	1.77 (↑ 90)
3	2.75 (↓ 23)	2.50 (↓ 30)	2.58 (↓ 28)	3.25 (↓ 9)	4.58 (↑ 28)	0.09 (↓ 90)	0.21 (↓ 77)	0.68 (↓ 27)	1.10 (↑ 18)	1.77 (↑ 90)

Table 3. EERs on the test set, for DTW and DTW + SL.

	Skilled	Random
DTW	5.80	1.07
DTW + SL	4.77 (↓ 18)	0.50 (↓ 53)

skilled impostor and $100 \times 99 = 9,900$ random impostor scores are considered for these experiments.

In the first step, a threshold δ is selected to tell random forgeries and genuine scores apart. The optimum value for δ is selected as the crossing point of the Joint-False Acceptance (JFAR) and False Rejection Rates (FRR), depicted in Fig. 2, where JFAR denotes a FAR comprising both skilled and random forgeries scores. As it may be observed, the crossing point is marked with a vertical line at 4, thus setting $\delta = 4$ for the remaining experiments.

After fixing δ, the performance of the global system is evaluated in terms of the EER, for different values of W_{fg} and W_{gen}, so that the optimum values are found. The ranges were empirically selected for both weights: outside those ranges, performance under one of the forgeries scenarios considerably drops. Results are shown in Table 2, where the EER for each considered set of parameters is included as well as the relative difference with respect to the baseline. $\mathrm{EER}_{\mathrm{sk}} = 3.58\%$ denotes the EER under the skilled forgeries scenario for the baseline, and, equivalently, $\mathrm{EER}_{\mathrm{rd}} = 0.93\%$ denotes the EER for the random forgeries.

Two different trends may be observed in Table 2: $i)$ under both forgeries scenarios, the bigger W_{fg}, the better the performance, reaching a bottom limit for $W_{fg} = 1.7$; $ii)$ whereas under the random forgeries scenario, the smaller the value of W_{gen}, the better (i.e., optimum found at $W_{gen} = 0$), for skilled forgeries, the best performance is reached for $W_{gen} = 0.1$. Taking these two considerations into account, a balance should be reached where the performance is at its best under both scenarios. As it may be seen in Table 2, a good balance is achieved for $W_{fg} \geq 1.7$, $W_{gen} = 0.1$.

4.3. Step 3: Performance Evaluation

Finally, in order to evaluate the performance of the full verification system, the test set is used (see Fig. 1 right). As mentioned in Sect. 3, $250 \times 12 = 3,000$ genuine, $250 \times 12 = 3,000$ skilled impostor and $250 \times 249 = 62,250$ random impostor scores are computed. These sets of scores are used to compute the Detection Error Trade-off (DET) curves in the random and impostor scenarios depicted in Fig. 3 and the corresponding EERs are summarized in Table 3. Also the distributions corresponding to these three sets of scores are depicted in Fig. 4, both for the case of the original DTW

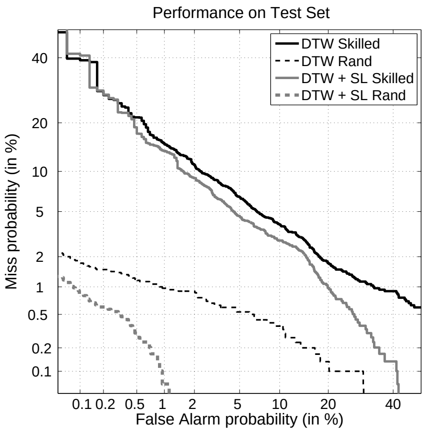

Figure 3. DET curves for the DTW baseline system and the full system (denoted DTW + SL) over the test set.

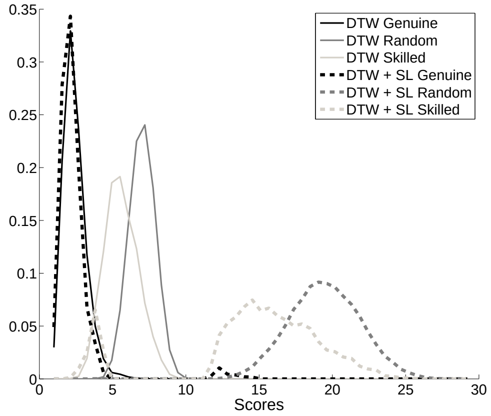

Figure 4. Score distributions before (solid lines) and after (dashed lines) applying the skilled detection module.

system and for the improved DTW-SL scheme proposed.

As it may be observed in Fig. 3, verification performance is improved at all operating points, this improvement being 36% on average at the EER. This performance improvement may be also observed in the bigger distance between the scores distributions in Fig. 4, where the S_{DTW} scores are depicted in solid lines, and their corresponding weighted scores S in dashed lines. It should be noted that, in the previous works using the same database and protocol, the performance achieved was lower (i.e., higher EERs). In [1], an HMM-based online signature verification system achieves EERs over 9%. Similarly, in [2], if just online information is considered, $\text{EER}_{\text{sk}} = 2.88\%$ and $\text{EER}_{\text{rd}} = 5.83\%$ are reported.

5. Conclusions

In the present article, a new enhanced and efficient online signature verification system has been proposed. A skilled forgery detector, fitting a multivariate Gaussian to each class (namely, genuine signatures and skilled forgeries) was trained with Sigma LogNormal features, and its output used to adapt the initial score emitted by the original verification system. It should be noted that this scheme requires skilled forgeries to train the skilled detector. Even if it is a requirement not needed by classical verification systems, this is not a too-strong assumption as there are public databases providing such data.

Experiments were carried out on the on-line signature corpus of the publicly available BiosecurID multimodal database. The database was divided into three independent sets so that results were not biased. Results showed improvements at all operating points, reaching around a 36% improvement at the EER.

As future work lines we consider the improvement of the skilled detector as this is the key for the increase of the performance of the complete system. Also the fusion of the knowledge provided by the skilled detector and the verification score will be improved, following the examples of previous works on anti-spoofing and verification systems fusion in [4, 14], where different sequential- and classifier-based approaches, as well as decision- and score-level fusion of anti-spoofing and verification systems, for face and fingerprint, are explored. Other signature matchers and databases will be taken into account as well.

6. Acknowledgements

This work has been partially supported by project Bio-Shield (TEC2012-34881) from Spanish MINECO, BEAT (FP7-SEC-284989) from EU, *Cátedra UAM-Telefónica*, *CECABANK*, and grant RGPIN-915 from NSERC Canada. M. G.-B. is supported by a FPU Fellowship from Spanish MECD.

References

[1] F. Alonso-Fernandez, J. Fierrez, et al. Robustness of signature verification systems to imitators with increasing skills. In *Proc. ICDAR*, pages 728–732, 2009.

[2] F. Alonso-Fernandez, J. Fierrez-Aguilar, et al. Fusion of static image and dynamic information for signature verification. In *Proc. ICIP*, 2009.

[3] V. Blankers, C. Heuvel, et al. ICDAR 2009 signature verification competition. In *Proc. ICDAR*, pages 1403–1407, 2009.

[4] I. Chingovska, A. Anjos, and S. Marcel. Anti-spoofing in action: joint operation with a verification system. In *Proc. CVPRW*, pages 98–104, 2013.

[5] J. Fierrez, J. Galbally, et al. BiosecurID: a multimodal biometric database. *Pattern Anal. and App.*, 13:235–246, 2009.

[6] J. K. Guo, D. Doermann, and A. Rosenfeld. Off-line skilled forgery detection using stroke and sub-stroke properties. In *Proc. ICPR*, volume 2, pages 355–358, 2000.

[7] J. K. Guo, D. Doermann, and A. Rosenfeld. Forgery detection by local correspondence. *IJPRAI*, 15(4):579–641, 2001.

[8] A. Hassaïne and S. Al-Maadeed. An online signature verification system for forgery and disguise detection. In *Neural Inf. Proc.*, pages 552–559, 2012.

[9] N. Houmani, A. Mayoue, et al. Biosecure signature evaluation campaign (BSEC-2009): Evaluating online signature algorithms depending on the quality of signatures. *Pattern Recognition*, 45(3):993–1003, 2012.

[10] M. Liwicki, M. I. Malik, et al. Signature verification competition for online and offline skilled forgeries (SigComp2011). In *Proc. ICDAR*, pages 1480–1484, 2011.

[11] M. Liwicki, C. E. van den Heuvel, et al. Forensic signature verification competition 4NSigComp2010 - detection of simulated and disguised signatures. In *Proc. ICFHR*, pages 715–720, 2010.

[12] V. K. Madasu and B. C. Lovell. An automatic offline signature verification and forgery detection system. *Pattern Rec. Tech. and App.: Recent Advances*, pages 63–89, 2008.

[13] M. Malik, M. Liwicki, et al. ICDAR 2013 competitions on signature verification and writer identification for on- and offline skilled forgeries (SigWiComp2013). In *Proc. ICDAR*, pages 1477–1483, 2013.

[14] E. Marasco, Y. Ding, and A. Ross. Combining match scores with liveness values in a fingerprint verification system. In *Proc. BTAS*, pages 418–425, 2012.

[15] M. Martinez-Diaz, J. Fierrez, R. P. Krish, and J. Galbally. Mobile signature verification: Feature robustness and performance comparison. *IET Biometrics*, 3:267–277, 20114.

[16] C. O'Reilly and R. Plamondon. Development of a sigma-lognormal representation for on-line signatures. *Pattern Recognition*, 42:3324–3337, 2009.