Complexity-based Biometric Signature Verification

Ruben Tolosana*, Ruben Vera-Rodriguez*, Richard Guest†, Julian Fierrez* and Javier Ortega-Garcia*
*Biometrics and Data Pattern Analytics (BiDA) Lab - ATVS, Escuela Politecnica Superior, Universidad Autonoma de Madrid
Avda. Francisco Tomas y Valiente, 11 - Campus de Cantoblanco - 28049 Madrid, Spain
Email: (ruben.tolosana, ruben.vera, julian.fierrez, javier.ortega)@uam.es
†School of Engineering and Digital Arts, University of Kent
Jennison Building, Canterbury CT2 7NT, UK
Email: R.M.Guest@kent.ac.uk

***Abstract*—On-line signature verification systems are mainly based on two approaches: feature- or time functions-based systems (a.k.a. global and local systems). However, new sources of information can be also considered in order to complement these traditional approaches, reduce the intra-class variability and achieve more robust signature verification systems against forgers. In this paper we focus on the use of the concept of complexity in on-line signature verification systems. The main contributions of the present work are: 1) classification of users according to the complexity level of their signatures using features extracted from the Sigma LogNormal writing generation model, and 2) a new architecture for signature verification exploiting signature complexity that results in highly improved performance. Our proposed approach is tested considering the BiosecurID on-line signature database with a total of 400 users. Results of 5.8% FRR for a FAR = 5.0% have been achieved against skilled forgeries outperforming recent related works. In addition, an analysis of the optimal time functions for each complexity level is performed providing practical insights for the application of signature verification in real scenarios.**

I. Introduction

On-line signature verification is experiencing high development due to the technological evolution of digitizing devices, including smartphones, and also as it finds application in many different sectors such as security, e-government, healthcare, education or banking [1], [2]. Two main approaches have been considered in on-line signature verification: 1) feature-based systems (a.k.a. global systems), and 2) time functions-based systems (a.k.a. local systems). While global systems are based on a set of features extracted from a signature, local systems consider whole time sequences providing more discriminant information and generally resulting in better system performance results [3].

New sources of information have been analysed in recent years in order to complement the traditional global and local systems and therefore, reduce the intra-class variability and achieve more robust signature verification systems against forgers. In this sense, it is important to consider the high potential of systems based on information extracted from writing generation models. These models allow the analysis of features related to motor control processes and the neuromuscular response, providing complementary features to the traditional X and Y pen coordinates and pressure. One of the most well known writing generation models is the Sigma LogNormal model [4]. This model has recently been used in [5] and [6] with success. In [5] the authors proposed a skilled forgery detector using some features extracted from the Sigma LogNormal model whereas in [6], a new set of features was proposed achieving very good performance with few features and a system based on the Dynamic Time Warping algorithm (DTW). This model has been used not only for signature verification purposes but to monitor a range of neuromuscular diseases [7].

Another important source of information relates to the concept of complexity. Signature verification systems have been shown to be highly sensitive to signature complexity [8]. In [9], Alonso *et al.* evaluated the effect of the complexity and legibility of the signatures for off-line signature verification (i.e. signatures with no available dynamic information) pointing out the differences in performance for several matchers. Signature complexity has also been associated to the concept of entropy, defining entropy as the inherent information content of biometric samples [10], [11], [12]. In [13] a "personal entropy" measure based on Hidden Markov Models (HMM) was proposed in order to analyse the complexity and variability of on-line signatures regarding three different levels of entropy. In addition, the same authors have recently proposed in [14] a new metric known as "relative entropy" for classifying users into animal groups (see the biometric menagerie [15]) where skilled forgeries are also considered. Despite all the studies performed in the on-line signature trait, none of them have exploited, as far as we are aware, the concept of complexity in order to develop more robust and accurate on-line signature verification systems.

The main contributions of the current work are twofold, namely: 1) classification of users according to the complexity level of their signatures using features extracted from the Sigma LogNormal writing generation model, and 2) a new architecture for signature verification exploiting signature complexity that results in highly improved performance.

The remainder of the paper is organized as follows. In Sec. II, our proposed methods for improving on-line signature verification systems are described. Sec. III describes the BiosecurID on-line signature database considered in the experimental work. Sec. IV describes the experimental protocol and the results achieved. Finally, Sec. V draws the final conclusions

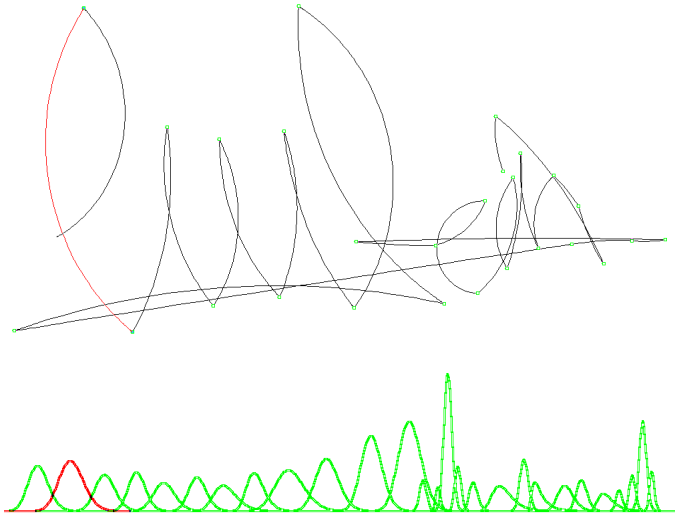

Fig. 1. Trace and velocity profile of one reconstructed on-line signature using the Sigma LogNormal model. A single stroke of the signature and its corresponding lognormal profile are highlighted in red colour. Individual strokes are segmented within the Sigma LogNormal algorithm [4].

and points out some lines for future work.

II. Proposed Methods

The main goal of this work is to enhance traditional on-line signature verification systems including information related to the concept of signature complexity and the Sigma LogNormal writing generation model. The following two stages are proposed in this work.

A. Signature Complexity Detector

This section describes the signature complexity detector proposed in this work. This detector is based on features extracted from the Sigma LogNormal model, which was first introduced to on-line signature in [4] and emulates the physiological model of human movement production for the generation of signatures. The idea of this approach is based on modelling one signature as a sum of single strokes in which each stroke has a lognormal velocity profile. Therefore, one signature can be modelled as follows:

$$\vec{v}(t) = \sum_{i=1}^{N} \vec{v_i}(t) \text{ with } N \geqslant 2 \quad (1)$$

where N represents the number of strokes involved in the generation of a given signature and $\vec{v_i}(t)$ is the lognomal velocity profile of the i-th stroke. Fig. 1 shows an example of the lognormal velocity profiles extracted for each stroke of one signature.

We propose to use the number of lognormals (N) that models each signature as a measure of the complexity level of the signature. Once this parameter is extracted for all available genuine signatures of the enrolment phase, the user is classified into a complexity level using the majority voting algorithm. Only genuine signatures are considered in our proposed approach for measuring the user signature complexity level. The advantage of this approach is that the signature complexity detector can be performed off-line thereby avoiding time consuming delays and making it feasible to apply in real time scenarios.

B. Complexity-based Signature Verification System

A separate on-line signature verification module based on time functions (a.k.a. local system) has been considered for each complexity level. For each signature acquired using a digitizing tablet (see Sec. III), signals related to *X* and *Y* pen coordinates and pressure are used to extract a set of 23 time functions, similar to [16] (see Table I). The more discriminative and robust time functions of each complexity level are selected using the Sequential Forward Feature Selection algorithm (SFFS) enhancing the signature verification system in terms of EER. The reason for the use of this time-function selection algorithm has been motivated due to the good results obtained in [17]. In that work the authors reduced the degradation of the system performance on device interoperability scenarios selecting the more robust features by the SFFS algorithm.

The local system considered in this work for computing the similarity between the time functions from the input and training signatures is based on the DTW algorithm. Scores are obtained as:

$$score = e^{-D/K} \quad (2)$$

where *D* and *K* represent respectively the minimal accumulated distance and the number of points aligned between two signatures using the DTW algorithm.

III. On-Line Signature Database

The BiosecurID database [18] was utilized in the experimental work of this paper. This database is comprised of 16 original signatures and 12 skilled forgeries per user, captured in 4 separate acquisition sessions leaving a two-month interval between them. There are a total of 400 users and signatures were acquired considering a controlled and supervised office-like scenario. Users were asked to sign on a piece of paper, inside a grid that marked the valid signing space, using an inking pen. The paper was placed on a Wacom Intuos 3 pen tablet that captured the following time signals of each signature: *X* and *Y* pen coordinates (0.25 mm resolution), pressure (1024 levels) and timestamp (100 Hz). In addition, pen-ups trajectories are available. All the dynamic information is stored in separate text files following the format used in the first Signature Verification Competition, SVC [19]. The signature acquisition process was supervised by a human operator whose task was to ensure that the collection protocol was strictly followed and that the captured samples were of sufficient quality (e.g. no part of the signature outside the designated space), otherwise, the donor was asked to repeat a given signature.

TABLE I
Set of time functions considered in this work.

#	Feature
1	x-coordinate: x_n
2	y-coordinate: y_n
3	Pen-pressure: z_n
4	Path-tangent angle: θ_n
5	Path velocity magnitude: v_n
6	Log curvature radius: ρ_n
7	Total acceleration magnitude: a_n
8-14	First-order derivate of features 1-7: $\dot{x_n}, \dot{y_n}, \dot{z_n}, \dot{\theta_n}, \dot{v_n}, \dot{\rho_n}, \dot{a_n}$
15-16	Second-order derivate of features 1-2: $\ddot{x_n}, \ddot{y_n}$
17	Ratio of the minimum over the maximum speed over a 5-samples window: v_n^r
18-19	Angle of consecutive samples and first order difference: α_n, $\dot{\alpha_n}$
20	Sine: s_n
21	Cosine: c_n
22	Stroke length to width ratio over a 5-samples window: r_n^5
23	Stroke length to width ratio over a 7-samples window: r_n^7

IV. Experimental Work

A. Experimental Protocol

The experimental protocol has been designed to allow the study of different complexity levels in the system performance. Two main experiments are carried out: 1) evaluation of the signature complexity detector proposed in this work in order to classify users into different complexity levels, and 2) evaluation of the proposed approach based on a different on-line signature verification system for each signature complexity level.

In the first experiment (Sec. IV-B1), all genuine signatures of BiosecurID database are considered in order to generate the probability density function of the number of lognormals and select three possible signature complexity levels. This was achieved following the same experimental protocol carried out in previous related works [13], [14]. It is important to highlight that in our proposed signature complexity detector, each user is classified into a complexity level group extracting only the number of lognormals of the enrolment signatures and then using the majority voting algorithm for classification, which does not require any training, so this does not introduce any bias in the evaluation results. In the second experiment (Sec. IV-B2 and IV-B3), the BiosecurID database is split into development dataset (40% of the users) and evaluation dataset (the remaining 60% of the users). The development dataset is considered in order to select the most discriminative and robust time functions for each signature complexity level using the SFFS algorithm whereas the evaluation dataset is considered for the evaluation of the proposed system.

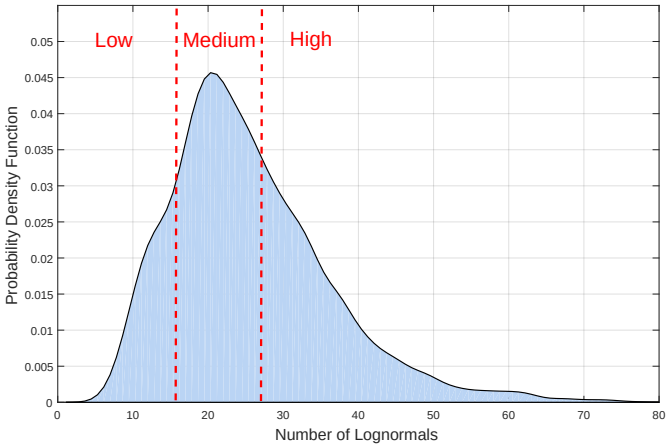

Fig. 2. Probability density function of the number of lognormals for all genuine signatures across BiosecurID database. The three proposed complexity-dependent decision thresholds are highlighted by red dashed lines.

For the analysis of our proposed signature complexity detector (Sec. IV-B1), and the development and evaluation of our proposed complexity-based signature verification systems (Sec. IV-B2 and Sec. IV-B3), the 4 genuine signatures of the first session are used as reference signatures, whereas the remaining genuine signatures (i.e. 12) are used for testing. Skilled forgery scores are obtained by comparing the reference signatures against the available skilled forgeries for each user (i.e. 12) whereas random (zero-effort) forgery scores are obtained by comparing the reference signatures with one genuine signature of each of the remaining users. The final score is obtained after performing the average score of the four one-to-one comparisons.

B. Experimental Results

*1) **Analysis of the Signature Complexity Detector**:* The signature complexity detector proposed in this work is based on the use of decision thresholding techniques. These techniques were successfully applied in [8] for score normalization.

The signature complexity detector is performed in two different steps. First, the Sigma LogNormal parameter N (see Sec. II-A) is extracted for each available genuine signature (i.e. a total of $400 \times 16 = 6400$ genuine signatures). Following this stage, lognormals from all genuine signatures are automatically classified into three signature complexity levels (low, medium and high) using K-means algorithm with $k = 3$ as proposed in [14]. Finally, the resulting signature complexity has been manually assessed and slightly adjusted to generate the final complexity-dependent decision thresholds. Fig. 2 shows the distribution of the number of lognormals for all genuine signatures across the BiosecurID database and the three proposed complexity-dependent decision thresholds. Signatures with lognormal values equal or less than 17 are classified as low-complexity signatures whereas those signatures with more than 27 lognormals are classified into the high-complexity group. Otherwise, signatures are categorized into

Fig. 3. Signatures from the BiosecurID database categorized for each complexity level using our proposed signature complexity detector.

TABLE II
EXPERIMENT 1: SYSTEM PERFORMANCE RESULTS (EER IN %) OF THE BIOSECURID DATABASE FOR EACH SIGNATURE COMPLEXITY LEVEL.

	Low C.	Medium C.	High C.
Skilled forgeries	22.2	21.7	17.9
Random forgeries	3.6	2.4	2.6

medium-complexity level. Fig. 3 shows some of the signatures classified into each complexity level. Our proposed signature complexity detector has obtained similar results compared to previous works: signatures with a high complexity level tend to be longer in writing time and have a more similar appearance to handwriting. However, signatures classified into a low complexity level are shorter in time and are generally simple flourish with no legible information.

We now analyse each resulting complexity level following the same procedure proposed in [14]: analysing the system performance with only X and Y pen coordinates for different complexity groups. It is important to remark that each user is classified into a complexity level applying the majority voting algorithm to all available enrolment signatures of the user (see Sec. II-A). Fig. 4 shows the system performance in terms of DET curves for each signature complexity level. In addition, Table II shows the system performance obtained for each complexity level in terms of EER(%).

The results show different system performance regarding the signature complexity level. Users with a high complexity level have an absolute improvement of 4.3% compared to users categorized into a low complexity level for skilled forgeries. Therefore, the idea of considering a different optimal on-line signature verification system for each signature complexity level is analysed in the following sections in order to select the most discriminative and robust time functions for each complexity group and reduce the system performance.

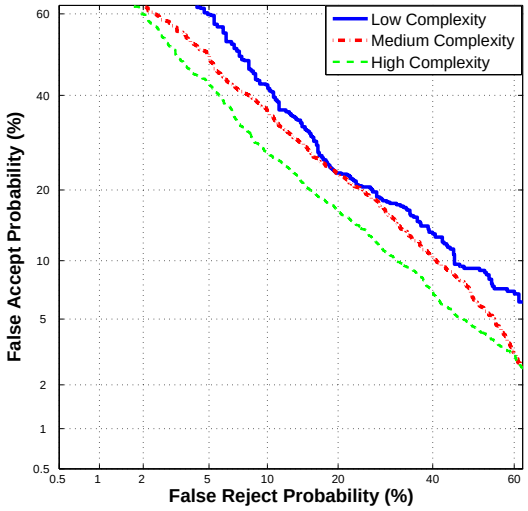

Fig. 4. **Experiment 1:** System performance of each signature complexity level considering skilled forgeries.

*2) **Time-Functions Selection for the Complexity-based Signature Verification System**:* First we analyse which are the most discriminative and robust time functions for each signature complexity level using the SFFS algorithm over the development dataset as it is described in Sec. II-B. The following three cases are studied:

1) Time functions selected for all three signature complexity levels.
2) Time functions selected only for medium and high signature complexity levels.
3) Time functions selected only for low and medium signature complexity levels.

For the first case, the time functions $\dot{z_n}$, $\dot{a_n}$ and v_n^r (see Table I) have been selected in all systems as robust time

TABLE III
EXPERIMENT 2: SYSTEM PERFORMANCE RESULTS (EER IN %) ON THE EVALUATION DATASET FOR EACH SIGNATURE COMPLEXITY LEVEL.

	Low C.		Medium C.		High C.	
	Baseline	Proposed	Baseline	Proposed	Baseline	Proposed
Skilled forgeries	13.8	10.1	7.5	5.2	6.2	4.6
Random forgeries	1.5	1.3	0.7	0.5	0.9	0.9

functions regardless of the signature complexity level. These time functions are the variation of pressure, variation of acceleration and ratio of the minimum over the maximum speed and provide general and valuable information to all signature verification systems about the knowledge and speed of the users performing their signatures. For the second case, the time functions $\dot{v_n}$, $\ddot{y_n}$ and $\dot{\alpha_n}$ have been selected for both medium and high signature complexity levels. These time functions provide information related to the variation of the velocity, vertical acceleration and variation of angle, time functions more related to the geometry of characters and therefore, with the handwriting. Finally, the time function c_n is the only one selected for the third case and provides information related to the angles as signatures with low and medium complexity level are usually categorized for having simple flourishes with no legible information. It is important to highlight that the time function $\ddot{y_n}$ is not selected for users with low signature complexity level. In other studies [20], [21], this time function was selected in most optimal systems. However, the vertical acceleration seems not to be very discriminative for users with low signature complexity level as their signatures are usually simpler and not related to handwriting.

*3) **Experimental Results of the Complexity-based Signature Verification System**:* In this section we evaluate our proposed approach based on the use of the signature complexity detector and the selection of the most discriminative time functions for each complexity level over the evaluation dataset. Table III shows the results achieved using our Proposed Systems. In order to make comparable our approach proposed in this work, we have used the same Baseline System recently studied in [5] and based on the use of the DTW algorithm with a total of 9 fixed time functions. The only two differences between the Proposed and Baseline Systems in Table III are: 1) the signature complexity detector, and 2) selection of time functions for each complexity level.

Analysing the results obtained, our Proposed Systems achieve an average absolute improvement of 2.5% EER compared to the Baseline System for the case of skilled forgeries. It is important to note that for the most challenging users (users with low signature complexity level), our proposed approach achieves an absolute improvement of 3.7% EER compared to the Baseline System. For completeness, Fig. 5 shows two examples of errors of our proposed system. First, a genuine comparison detected as a forgery, and second a skilled forgery test detected as a genuine signature. Analysing the results obtained for the random forgery cases, our Proposed Systems also achieve improvements for all complexity levels. For this

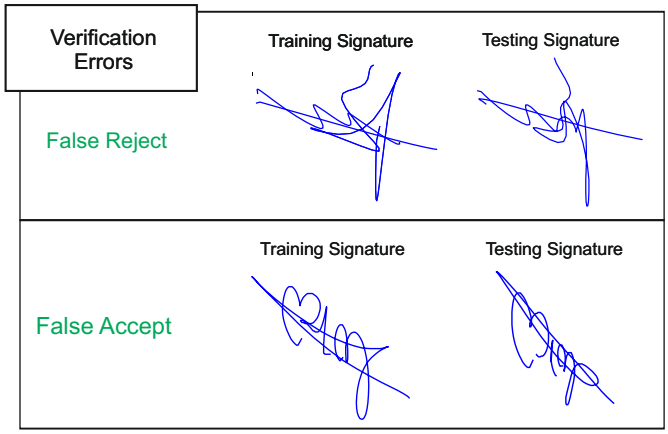

Fig. 5. **Experiment 2:** Genuine (top) and impostor (bottom) comparisons detected by the system as impostor and genuine, respectively.

case, the improvement has been lower than for skilled forgery cases due to its low values and the way that the SFFS algorithm was applied during the training of the systems (focused on skilled forgery cases). Therefore, the results obtained after applying our proposed approach based on complexity-based signature verification systems have outperformed the state-of-the-art results for the BiosecurID database [5], [22].

For completeness, Fig. 6 shows the performance of the Baseline and Proposed Systems considering all complexity levels together in terms of the false rejection rate (FRR) at different values of false acceptance rate (FAR). Our Proposed Systems achieve a final value of 5.8% FRR for a FAR = 5.0% and 3.9% FRR for a FAR = 10.0%. These results show the importance of considering different signature verification systems for each signature complexity level in order to enhance the verification systems with more robust time functions.

V. CONCLUSIONS

In this paper the concept of complexity is exploited in order to improve the traditional approaches in on-line signature verification. A new methodology based on the two following stages is proposed: 1) classification of users according to the complexity level of their signatures using features extracted from the Sigma LogNormal writing generation model, and 2) a new architecture for signature verification exploiting signature complexity that results in highly improved performance. Our proposed approach has been analysed considering the BiosecurID on-line signature database with a total of 400 users.

Our Proposed Systems have achieved an average absolute improvement of 2.5% EER compared to the Baseline System

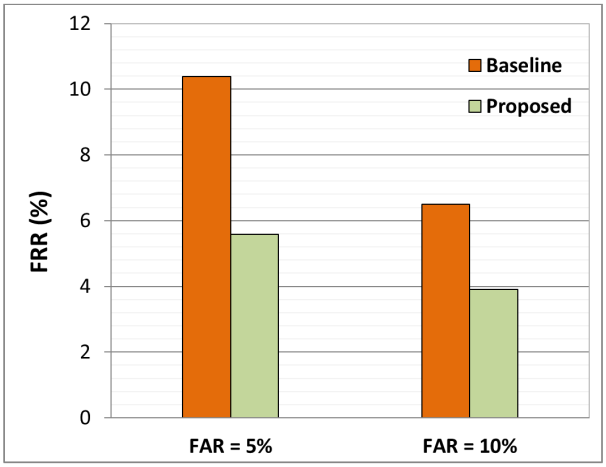

Fig. 6. **Experiment 2:** Analysis of the False Rejection Rate (FRR) at different values of the False Acceptance Rate (FAR) for the Baseline and the Proposed Systems on the whole evaluation dataset.

for the case of skilled forgeries. It is important to note that for the most challenging users (users with low signature complexity level), our proposed approach has achieved an absolute improvement of 3.7% EER compared to the Baseline System. Finally, for the case of considering all complexity levels together, our Proposed Systems have achieved a final value of 5.8% FRR for a FAR = 5.0%. These results have outperformed the state-of-the-art. In addition, an evaluation of the most discriminative and robust time functions of each signature complexity level has been carried out pointing out some practical insights for the application of signature verification in practical scenarios.

For future work, the approach considered in this work will be further analysed using the e-BioSign public database [23] in order to consider new scenarios such as the case of using the finger as the writing tool or the case of acquiring signatures using independently the stylus or the finger as the writing tool (i.e. mixed writing-tool scenarios).

ACKNOWLEDGMENTS

This work has been supported by project TEC2015-70627-R MINECO/FEDER and by UAM-CecaBank Project. Ruben Tolosana is supported by a FPU Fellowship from Spanish MECD.

REFERENCES

[1] R. Plamondon, G. Pirlo and D. Impedovo, "Online signature verification," D. Doermann and K. Tombre (Eds.), *Handbook of Document Image Processing and Recognition*, Springer, pp. 917-947, 2014.

[2] R. Guest, "Age Dependency in Handwritten Dynamic Signature Verification Systems," *Pattern Recognition Letters*, vol. 27, no. 10, pp. 1098–1104, 2006.

[3] M. Martinez-Diaz, J. Fierrez and S. Hangai, "Signature features," S.Z. Li and A. Jain (Eds.), *Encyclopedia of Biometrics*, Springer, pp. 1375-1382, 2015.

[4] C. O'Reilly and R. Plamondon, "Development of a Sigma-Lognormal Representation for On-Line Signatures," *Pattern Recognition*, vol. 42, no. 12, pp. 3324–3337, 2009.

[5] M. Gomez-Barrero, J. Galbally, J. Fierrez, J. Ortega-Garcia and R. Plamondon, "Enhanced On-Line Signature Verification Based on Skilled Forgery Detection Using Sigma-LogNormal Features," in *Proc. IEEE/IAPR Int. Conf. on Biometrics, ICB*, 2015, pp. 501–506.

[6] A. Fischer and R. Plamondon, "Signature Verification Based on the Kinematic Theory of Rapid Human Movements," in *IEEE Transactions on Human-Machine Systems*, 2016, pp. 1–12.

[7] D. Impedovo, G. Pirlo, F.M. Mangini, D. Barbuzzi, A. Rollo, A. Balestrucci, S. Impedovo, L. Sarcinella, C. O'Reilly and R. Plamondon, "Writing generation model for health care neuromuscular system investigation," E. Formenti, R. Tagliaferri and E. Wit (Eds.) , *Computational Intelligence Methods for Bioinformatics and Biostatistics*, Springer, pp. 137-148, 2014.

[8] J. Fierrez, J. Ortega-Garcia and J. Gonzalez-Rodriguez, "Target dependent score normalization techniques and their application to signature verification," *IEEE Transactions on Systems, Man, and Cybernetics. Part C*, vol. 35, no. 3, pp. 418–425, 2005.

[9] F. Alonso-Fernandez, M.C. Fairhurst, J. Fierrez and J. Ortega-Garcia, "Impact of Signature Legibility and Signature Type in Off-Line Signature Verification," *In Proc. IEEE Biometrics Symposium*, pp. 1–6, 2007.

[10] J. Daugman, "The Importance of Being Random: Statistical Principles of Iris Recognition," *Pattern Recognition*, vol. 36, no. 2, pp. 279–291, 2003.

[11] M. Lim and P. Yuen, "Entropy Measurement for Biometric Verification Systems," *IEEE Transactions on Cybernetics*, vol. 46, no. 5, pp. 1065–1077, 2016.

[12] Z.H. Zhou, "Biometric entropy," S.Z. Li and A. Jain (Eds.), *Encyclopedia of Biometrics*, Springer, pp. 273-274, 2009.

[13] N. Houmani, S. Garcia-Salicetti and B. Dorizzi, "A Novel Personal Entropy Measure Confronted to Online Signature Verification Systems Performance," *In Proc. Intl. Conf.on Biometrics : Theory, Applications and System, BTAS*, pp. 1–6, 2008.

[14] N. Houmani and S. Garcia-Salicetti, "On Hunting Animals of the Biometric Menagerie for Online Signature," *PLOS ONE*, vol. 11, no. 4, 2016.

[15] N. Yager and T. Dunstone, "The Biometric Menagerie," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 2, pp. 220–230, 2010.

[16] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia and J. Fierrez, "Update Strategies for HMM-Based Dynamic Signature Biometric Systems," in *Proc. 7th IEEE Int. Workshop on Information Forensics and Security*, 2015.

[17] R. Tolosana, R. Vera-Rodriguez, J. Ortega-Garcia, and J. Fierrez, "Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification," *IEEE Access*, vol. 3, pp. 478–489, May 2015.

[18] J. Fierrez, *et al.*, "BiosecurID: A Multimodal Biometric Database," *Pattern Analysis and Applications*, vol. 13, no. 2, pp. 235–246, May 2010.

[19] D.Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto and G. Rigoll, "SVC2004: First International Signature Verification Competition," *In Proc. IAPR Int. Conf. on Biometric Authentication. Springer.*, no. 3072, pp. 16–22, 2004.

[20] M. Martinez-Diaz, J. Fierrez and J. Galbally, "Graphical Password-Based User Authentication With Free-Form Doodles," *IEEE Transactions on Human-Machine Systems*, vol. 46, no. 4, pp. 607–614, 2016.

[21] M. Martinez-Diaz and J. Fierrez and R. P. Krish and J. Galbally, "Mobile Signature Verification: Feature Robustness and Performance Comparison," *IET Biometrics*, vol. 3, no. 4, pp. 267–277, 2014.

[22] F. Alonso-Fernandez, J. Fierrez, A. Gilperez, J. Galbally and J. Ortega-Garcia, "Robustness of Signature Verification Systems to Imitators with Increasing Skills," *In Proc. 10th Int. Conf. on Document Analysis and Recognition*, p. 728732, 2009.

[23] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales and J. Ortega-Garcia, "Benchmarking Desktop and Mobile Handwriting across COTS Devices: the e-BioSign Biometric Database," *PLOS ONE*, 2017.