Do You Need More Data? The DeepSignDB On-Line Handwritten Signature Biometric Database

Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia
Biometrics and Data Pattern Analytics - BiDA Lab, Universidad Autonoma de Madrid
{ruben.tolosana, ruben.vera, julian.fierrez, aythami.morales, javier.ortega}@uam.es

***Abstract*—Data have become one of the most valuable things in this new era where deep learning technology seems to overcome traditional approaches. However, in some tasks, such as the verification of handwritten signatures, the amount of publicly available data is scarce, what makes difficult to test the real limits of deep learning. In addition to the lack of public data, it is not easy to evaluate the improvements of novel approaches compared with the state of the art as different experimental protocols and conditions are usually considered for different signature databases. To tackle all these mentioned problems, the main contribution of this study is twofold: *i)* we present and describe the new DeepSignDB on-line handwritten signature biometric public database, and *ii)* we propose a standard experimental protocol and benchmark to be used for the research community in order to perform a fair comparison of novel approaches with the state of the art. The DeepSignDB database is obtained through the combination of some of the most popular on-line signature databases, and a novel dataset not presented yet. It comprises more than 70K signatures acquired using both stylus and finger inputs from a total of 1526 users. Two acquisition scenarios are considered, office and mobile, with a total of 8 different devices. Additionally, different types of impostors and number of acquisition sessions are considered along the database. The DeepSignDB and benchmark results are available in GitHub[1].**

***Index Terms*—biometrics, handwritten signature, DeepSignDB database, deep learning, RNN, DTW**

I. Introduction

On-line handwritten signature verification has widely evolved in the last 40 years [1]. From the original Wacom devices specifically designed to acquire handwriting and signature in office-like scenarios to the current mobile acquisition scenarios in which signatures can be captured using our own personal smartphone anywhere [2]. However, and despite the improvements achieved in the acquisition technology, the core of most of the state-of-the-art signature verification systems is still based on traditional approaches such as Dynamic Time Warping (DTW), Hidden Markov Models (HMM), and Support Vector Machines (SVM). This aspect seems to be a bit unusual if we compare to other biometric traits such as face and fingerprint in which Deep Learning (DL) has defeated by far traditional approaches [3], [4], and even in tasks more related to signature verification such as handwriting recognition or writer verification [5], [6]. So, why DL approaches are not widely used in on-line signature verification yet? One major handicap could be probably the complex procedure of acquiring a large-scale database for training the models as signatures are not publicly available on internet as it happens with other biometric traits such as the face [7].

In addition to the scarcity of data for training DL approaches, another important observation motivates this work: the lack of a standard experimental protocol to be used for the research community in order to perform a fair comparison of novel approaches to the state of the art, as different experimental protocols and conditions are usually considered for different signature databases [8], [9]. With all these concerns in mind, in this study we present the new DeepSignDB handwritten signature biometric database, the largest on-line signature database to date. Fig. 1 graphically summarises the design, acquisition devices, and writing tools considered in the DeepSignDB database. Its application extends from the improvement of signature verification systems via deep learning to many other potential research lines, e.g., studying: *i)* user-dependent effects, and development of user-dependent methods in signature biometrics, and handwriting recognition at large [10], *ii)* the neuromotor processes involved in signature biometrics [11], and handwriting in general [12], *iii)* sensing factors in obtaining representative and clean handwriting and touch interaction signals [13], *iv)* human-device interaction factors involving handwriting and touchscreen signals [14], and development of improved interaction methods [15], and *v)* population statistics around handwriting and touch interaction signals, and development of new methods aimed at recognising or serving particular population groups [16], [17].

The main contributions of this study can be summarised as follows:

- We present and describe the new DeepSignDB on-line handwritten signature database. This database is obtained through the combination of some of the most well-known databases, and a novel dataset not presented yet. It comprises more than 70K signatures acquired using both stylus and finger inputs from a total 1526 users. Two acquisition scenarios are considered, office and mobile, with a total of 8 different devices. Additionally, different types of impostors and number of acquisition sessions are considered along the database.
- We propose a standard experimental protocol to be used for the research community in order to perform a fair comparison of novel approaches to the state of the art. Thus, we also release the files with all the signature comparisons carried out using the final evaluation dataset. This way we provide an easily reproducible framework.

[1] https://github.com/BiDAlab/DeepSignDB

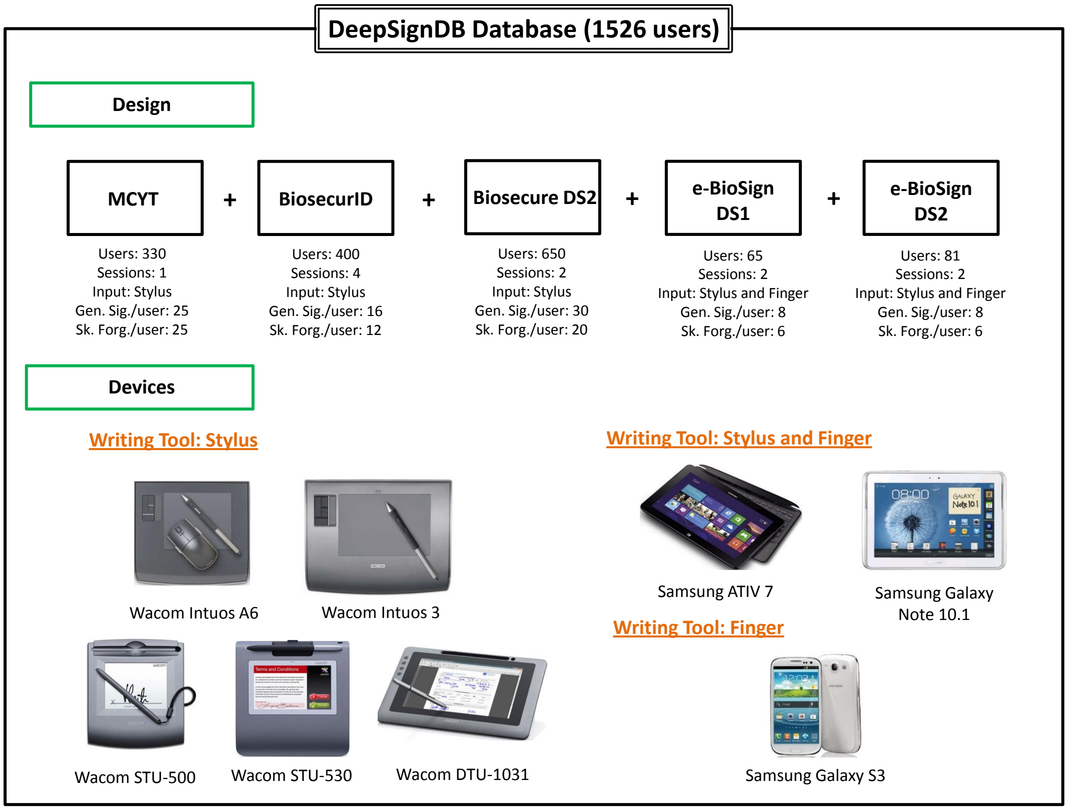


Fig. 1: Description of the design, acquisition devices, and writing tools considered in the new DeepSignDB database. A total of 1526 users and 8 different captured devices are used (5 Wacom and 3 Samsung general purpose devices). For the Samsung devices, signatures are also collected using the finger. Gen. Sig. = Genuine Signatures, and Sk. Forg. = Skilled Forgeries.

TABLE I: Total number of users and signatures considered in the DeepSignDB database for training the networks compared to previous studies.

Work	# Users	# Signatures
Otte *et al.* [18]	20	∼1K
Tolosana *et al.* [19]	300	∼8K
Lai and Jin [20]	193	∼9K
DeepSignDB Database	**1084**	**∼50K**

- We report a benchmark evaluation of the new DeepSignDB database considering a state-of-the-art system based on DTW and DL.

The remainder of the paper is organised as follows. Sec. II summarises previous studies carried out in on-line signature verification via DL. Sec. III describes the design of the DeepSignDB signature database. Sec. IV describes the proposed experimental protocol, and the benchmark evaluation carried out using a state-of-the-art signature verification system. Finally, Sec. V draws the final conclusions and points out some lines for future work.

II. On-Line Signature Verification Via Deep Learning

Despite the lack of data, some authors have preliminary evaluated the potential of Recurrent Neural Networks (RNNs), which is a specific DL architecture used for modelling sequential data with arbitrary length, for on-line signature verification. Table I depicts the total number of users and signatures considered in the DeepSignDB database for training the networks compared to previous studies. In [18], the authors performed an exhaustive analysis of Long Short-Term Memory (LSTM) RNNs using a total of 20 users and ∼1K signatures for training. Three different scenarios were studied: *i)* training a general network to distinguish forgeries from genuine signatures, *ii)* training a different network for each writer, and *iii)* training the network using only genuine signatures. However, all experiments failed obtaining a final 23.75% EER for the best network configuration, far away from the state of the art, concluding that LSTM RNN systems trained with standard mechanisms were not appropriate for the task of signature verification as the amount of available data for this task is scarce compared to other tasks, e.g., handwriting recognition. More recently, some researchers have preliminary shown the potential of DL for the task of on-line signature verification through the design of new architectures. In [19], we proposed an end-to-end writer-independent RNN signature verification system based on a Siamese architecture. LSTM and Gated Recurrent Unit (GRU) RNNs were studied, using both normal and bidirectional configurations. For training the networks, we considered a total of 300 users and ∼8K signatures. Our proposed system outperformed a state-of-the-art signature verification system based on DTW and feature selection techniques for the case of skilled forgeries. However, the results achieved using that RNN system were not able to outperform the DTW system for the case of random forgeries. Finally, Lai and Jin proposed in [20] the use of GRU RNNs in combination with a novel descriptor named Length-Normalized Path Signature (LNPS). Experiments were carried out using a total of 193 users and ∼9K signatures for the training, analysing both skilled and random forgeries. The DeepSignDB database presented in this study increases in large numbers the users and signatures available for training the networks.

III. DeepSignDB Database Description

The DeepSignDB database comprises a total of 1526 users from four different popular databases (i.e., MCYT, BiosecurID, Biosecure DS2, and e-BioSign DS1) and a novel signature database not presented yet, named e-BioSign DS2. Fig. 1 graphically summarises the design, acquisition devices, and writing tools considered in the DeepSignDB database. A short description of each database regarding the device, writing input, number of acquisition sessions and time gap between them, and type of impostors [21] is now included for completeness. For more details we refer to their corresponding references.

A. MCYT

The MCYT database [22] comprises a total of 25 genuine signatures and 25 skilled forgeries per user, acquired in a single session in blocks of 5 signatures. There are a total of 330 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 A6 USB pen tablet that captured the following time signals: *X* and *Y* spatial coordinates (resolution of 0.25 mm), pressure (1024 levels), pen angular orientations (i.e., azimuth and altitude angles) and timestamps (100 Hz). In addition, pen-up trajectories are available.

Regarding the type of impostors, static forgeries were considered allowing forgers to have access only to the image of the signatures to be forged.

B. BiosecurID

The BiosecurID database [23] comprises a total of 16 genuine 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: *X* and *Y* spatial coordinates (resolution of 0.25 mm), pressure (1024 levels), pen angular orientations (i.e., azimuth and altitude angles) and timestamps (100 Hz). Pen-up trajectories are also available.

Regarding the type of impostors, both static and dynamic forgeries were considered: in the first two sessions forgers had access only to the image of the signature to be forged whereas in the last two sessions forgers had also access to the dynamics.

C. Biosecure DS2

The Biosecure DS2 database [24] comprises a total of 30 genuine signatures and 20 skilled forgeries per user, captured in 2 separate acquisition sessions leaving a three-month time interval between them. There are a total of 650 users and signatures were acquired considering a controlled and supervised office-like scenario. Users were asked to sign on a paper sheet placed on top of a Wacom Intuos 3 device while sitting. The same acquisition conditions were considered as per BiosecurID database.

Regarding the type of impostors, only dynamic forgeries were considered.

D. e-BioSign DS1

The e-BioSign DS1 database [2] is composed of five different devices. Three of them are specifically designed for capturing handwritten data (i.e., Wacom STU-500, STU-530, and DTU-1031), while the other two are general purpose tablets not designed for that specific task (Samsung ATIV 7 and Galaxy Note 10.1). It is worth noting that all five devices were used with their own pen stylus. Additionally, the two Samsung devices were used with the finger as input, allowing the analysis of the writing input on the system performance. The same capturing protocol was used for all five devices: devices were placed on a desktop and subjects were able to rotate them in order to feel comfortable with the writing position. The software for capturing handwriting and signatures was developed in the same way for all devices in order to minimise the variability of the user during the acquisition process.

Signatures were collected in two sessions for 65 subjects with a time gap between sessions of at least 3 weeks. For each user and writing input, there are a total of 8 genuine signatures and 6 skilled forgeries. For the case of using the stylus as input, information related to *X* and *Y* spatial coordinates, pressure and timestamp is recorded for all devices. In addition, pen-up trajectories are also available. However, pressure information and pen-up trajectories are not recorded when the finger is used as input.

Regarding the impostors, both dynamic and static forgeries were considered in the first and second acquisition sessions, respectively.

E. e-BioSign DS2

DeepSignDB database also includes a new on-line signature dataset not presented yet, named e-BioSign DS2. This dataset follows the same capturing protocol as e-BioSign DS1. Three different devices were considered: a Wacom STU-530 specifically designed for capturing handwritten data, a Samsung

TABLE II: Experimental protocol details of the DeepSignDB evaluation dataset (442 users). Numbers are per user and device.

STYLUS WRITING INPUT

Database	#Users	Devices	#Train Genuine Signatures	#Test Genuine Signatures	#Test Skilled Forgeries	#Test Random Forgeries
MCYT	100	Wacom Intuos A6	1/4 (Session 1)	21 (rest)	25 (all)	99 (one of the rest users)
BiosecurID	132	Wacom Intuos 3	1/4 (Session 1)	12 (Sessions 2-4)	12 (all)	131 (one of the rest users)
Biosecure DS2	140	Wacom Intuos 3	1/4 (Session 1)	15 (Session 2)	20 (all)	139 (one of the rest users)
e-BioSign DS1	35	Wacom STU-500 Wacom STU-530 Wacom DTU-1031 Samsung ATIV 7 Samsung Note 10.1	1/4 (Session 1)	4 (Session 2)	6 (all)	34 (one of the rest users)
e-BioSign DS2	35	Wacom STU-530	1/4 (Session 1)	4 (Session 2)	6 (all)	34 (one of the rest users)

FINGER WRITING INPUT

Database	#Users	Devices	#Train Genuine Signatures	#Test Genuine Signatures	#Test Skilled Forgeries	#Test Random Forgeries
e-BioSign DS1	35	Samsung ATIV 7 Samsung Note 10.1	1/4 (Session 1)	4 (Session 2)	6 (all)	34 (one of the rest users)
e-BioSign DS2	35	Samsung Note 10.1 Samsung S3	1/4 (Session 1)	4 (Session 2)	6 (all)	34 (one of the rest users)

Galaxy Note 10.1 general purpose tablet, and a Samsung Galaxy S3 smartphone. For the first device, signatures where captured using the stylus in an office-like scenario, i.e., the device was placed on a desktop and subjects were able to rotate it in order to feel comfortable with the writing position. For the Samsung Galaxy Note 10.1 tablet and Galaxy S3 smartphone, the finger was used as input. The acquisition conditions emulated a mobile scenario where users had to sign while sitting.

Signatures were collected in two sessions for 81 users with a time gap between sessions of at least 3 weeks. For each user, device, and writing input, there are a total of 8 genuine signatures and 6 skilled forgeries. For the case of using the stylus as input, information related to *X* and *Y* spatial coordinates, pressure and timestamp is recorded for all devices. In addition, pen-up trajectories are also available. However, pressure information and pen-ups trajectories are not recorded when the finger is used as input.

Regarding the type of impostors, only dynamic forgeries were considered, allowing forgers to have access to both image and dynamics of the signatures to be forged. In order to perform high quality forgeries, users were allowed to visualize a recording of the dynamic realization of the signature to forge as many times as they wanted.

IV. DeepSignDB Benchmark

This section reports the benchmark evaluation carried out for the DeepSignDB on-line handwritten signature database. Sec. IV-A describes all the details of our proposed experimental protocol to be used for the research community in order to facilitate the fair comparison of novel approaches to the state of the art. Then, Sec. IV-B describes the baseline signature verification system considered in the benchmark evaluation. Finally, we analyse the results obtained in Sec. IV-C.

A. Experimental Protocol

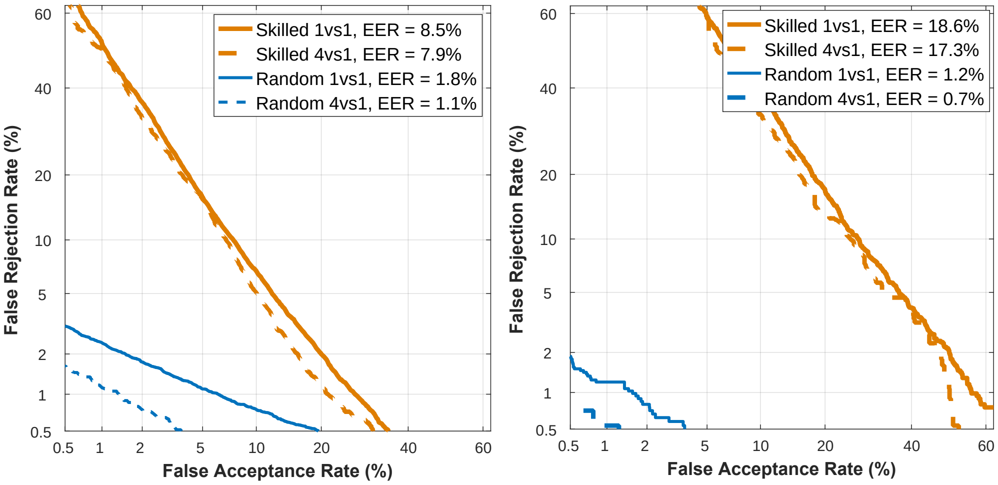
The DeepSignDB database has been divided into two different datasets, one for the development and training of the system and the other one for the final evaluation. The development dataset comprises around 70% of the users of each database whereas the remaining 30% are included in the evaluation dataset. It is important to note that each dataset comprises different users in order to avoid biased results. Thus, we first identified all those users that took part in the acquisition of different databases. Additionally, we corrected several mistakes we found along the different databases.

For the training of the systems, the development dataset comprises a total of 1084 users. In our experiments, we have divided this dataset into two different subsets, training (80%) and validation (20%). However, as this dataset is used only for development, and not for the final evaluation of the systems, we prefer not to set any restriction and let researchers use it as they like.

For the final testing of the systems, the remaining 442 users of the DeepSignDB database are included in the evaluation dataset. In order to perform a complete and fair analysis of the signature verification systems, and see their generalisation capacity to different scenarios, the following aspects have been considered in the final experimental protocol design:

- **Inter-session variability:** genuine signatures from different sessions are considered for training and testing (different acquisition blocks for the MCYT database).
- **Number of training signatures:** two different cases are considered, the case of having just one genuine signature from the first session (1vs1) or the case of using the first 4 genuine signatures from the first session (4vs1).
- **Impostor scenario:** skilled and random forgeries are considered in the experimental protocol. For the skilled forgery case, all available samples are included in the analysis whereas for the random forgery case, one genuine sample of each of the remaining users of the same database is considered. This way verification systems are tested with different types of presentation attacks [21].
- **Writing input:** stylus and finger scenarios are also considered in the experimental protocol due to the high acceptance of the society to use mobile devices on a daily basis [25].

Table II describes all the experimental protocol details of the DeepSignDB evaluation dataset for both stylus (top) and finger (bottom) writing inputs.



(a) Stylus

(b) Finger

Fig. 2: System performance results over the DeepSignDB evaluation dataset. (a) Stylus writing input. (b) Finger writing input.

B. Baseline Signature Verificastion System

For the benchmark evaluation of the DeepSignDB database, we have considered the same DTW and RNN signature verification systems presented in [19]. In that study, RNN approaches outperformed a DTW system for skilled forgeries. However, for random forgeries, DTW still outperformed RNNs with results very close to 0% EER. As a result, we propose in this benchmark a signature verification system based on the two following stages:

1) We first consider the same DTW system to detect random forgeries as it provides very good results against this type of attacks.
2) Then, in case the input signature is not detected as random forgery, it is moved forward to the second authentication stage based on a Bidirectional GRU (BGRU) signature verification system with a Siamese architecture [19]. This second stage is in charge of detecting skilled forgeries.

Finally, for the analysis of having 4 train genuine signatures (4vs1), the final score is obtained as the average score of the 4 one-to-one comparisons.

C. Experimental Results

Two different scenarios are evaluated. First, an office-like scenario where users perform their signatures using the stylus as input (Table II, top), and then a mobile scenario where users perform their signatures using the finger (Table II, bottom).

*1) **Stylus Writing Input Scenario**:* For the development of our baseline system, the weights of the BGRU system are trained using the development dataset composed of 1084 users. Only signatures acquired using the stylus are considered, ending up with around 309K genuine and impostor comparisons (247K and 62K for training and validation, respectively). It is important to remark: *i)* the same number of genuine and impostor comparisons are used to train the BGRU in order to avoid bias, and *ii)* only skilled forgeries are used as impostors (the DTW is in charge of detecting the random forgeries).

Fig. 2a shows the system performance results obtained using the DeepSignDB evaluation dataset for the stylus scenario. Analysing the skilled forgery case, the baseline system achieves 8.5% and 7.9% EERs for the 1vs1 and 4vs1 cases, respectively. For this specific impostor case, both DET curves are very similar despite having more training signatures per user (from one to four). We believe this is produced due to the limitations of our Siamese architecture as just a single train signature of the user is introduced in the system per comparison. Therefore, new DL architectures should be proposed for the research community to improve the system performance when having more available signatures.

Analysing the random forgery case, our baseline system achieves 1.8% and 1.1% EERs for the 1vs1 and 4vs1 cases, respectively. In this specific impostor case, a higher system performance improvement is achieved when increasing the training signatures from one to four. For a high convenient system with a False Rejection Rate (FRR) of 0.5%, a False Acceptance Rate (FAR) of 20% is achieved by the baseline system for the 1vs1 case. This FAR value improves to around 4% for the 4vs1 case, improving the security of the system against random attacks in large margins. These results show the potential of the first stage based on DTW against random forgeries.

*2) **Finger Writing Input Scenario**:* We consider the same baseline system trained in the previous section for the stylus input. This way we can: *i)* evaluate the generalisation capacity of the network to unseen scenarios, e.g., the finger, and *ii)* encourage all the research community to use the DeepSignDB database and explore new DL approaches such as transfer learning in this challenging scenario [26], [27].

Fig. 2b shows the system performance results obtained using the DeepSignDB evaluation dataset for the finger scenario. Analysing the skilled forgery case, the baseline system achieves 18.6% and 17.3% EERs for the 1vs1 and 4vs1 cases, respectively. Despite these results are higher than the same ones obtained in the stylus scenario, the baseline system has outperformed the original results obtained in [2], where one system was specifically trained per device.

Analysing the random forgery case, our baseline system achieves 1.2% and 0.7% EERs for the 1vs1 and 4vs1 cases, respectively. These results outperform the results achieved in the stylus scenario. For a high convenient system with a FRR = 0.5%, a FAR = 4% is achieved for the 1vs1 case, a FAR improvement of 16% compared to the stylus case. The same trend is observed for the 4vs1 case, achieving a FAR around 1% for a FRR = 0.5%.

V. Conclusions

In this paper we have presented the DeepSignDB on-line handwritten signature database, the largest on-line signature database to date. This database comprises more than 70K signatures acquired using both stylus and finger inputs from a total of 1526 users. Two acquisition scenarios are considered (i.e., office and mobile), with a total of 8 different devices. Additionally, different types of impostors and number of acquisition sessions are considered along the database.

In addition, we propose a standard experimental protocol and benchmark of the new DeepSignDB database using a state-of-the-art signature verification system. For the stylus scenario, results around 8% and 1-2% EERs have been obtained for skilled and random forgeries, respectively. Analysing the finger scenario, the same baseline system trained for the stylus case has been considered. Higher EERs have been obtained for skilled forgeries. However, a considerable system performance improvement is achieved compared to the stylus scenario for random forgeries.

For future work, we encourage all the research community to use DeepSignDB database for several purposes: *i)* perform a fair comparison of novel approaches to the state of the art, *ii)* evaluate the limits of novel DL architectures, and *iii)* carry out a more exhaustive analysis of the challenging finger input scenario.

Acknowledgments

This work has been supported by projects: BIBECA (RTI2018-101248-B-I00 MINECO/FEDER), Bio-Guard (Ayudas Fundación BBVA a Equipos de Investigación Científica 2017) and by UAM-CecaBank. Ruben Tolosana is supported by a FPU Fellowship from Spanish MECD.

References

[1] M. Diaz, M.A. Ferrer, D. Impedovo, M.I. Malik, G. Pirlo and R. Plamondon, “A Perspective Analysis of Handwritten Signature Technology,” *ACM Computing Surveys*, vol. 51, pp. 1–39, 2019.

[2] 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*, vol. 12, no. 5, pp. 1–17, 2017.

[3] K. Sundararajan and D. Woodard, “Deep Learning for Biometrics: A Survey,” *ACM Computing Surveys*, vol. 51, no. 3, pp. 1–34, 2018.

[4] M. Vatsa, R. Singh, and A. Majumdar, Eds., *Deep Learning in Biometrics*. CRC Press, 2018.

[5] A. Graves, M. Liwicki, S. Fernandez, R. Bertolami, H. Bunke, and J. Schmidhuber, “A Novel Connectionist System for Unconstrained Handwriting Recognition,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, no. 5, pp. 855–868, 2009.

[6] X. Zhang, G. Xie, C. Liu, and Y. Bengio, “End-to-End Online Writer Identification With Recurrent Neural Network,” *IEEE Transactions on Human-Machine Systems*, vol. 47, no. 2, pp. 285–292, 2017.

[7] I. Kemelmacher-Shlizerman, S. Seitz, D. Miller, and E. Brossard, “The Megaface Benchmark: 1 Million Faces for Recognition at Scale,” in *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition*, 2016, pp. 4873–4882.

[8] M. Diaz, A. Fischer, M.A. Ferrer and R. Plamondon, “Dynamic Signature Verification System based on One Real Signature,” *IEEE Transactions on Cybernetics*, vol. 48, no. 1, pp. 228–239, 2018.

[9] Y. Liu, Z. Yang, and L. Yang, “Online Signature Verification based on DCT and Sparse Representation,” *IEEE Transactions on Cybernetics*, vol. 45, no. 11, pp. 2498–2511, 2015.

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

[11] R. Vera-Rodriguez, R. Tolosana, and *et al.*, “Modeling the Complexity of Signature and Touch-Screen Biometrics using the Lognormality Principle,” *R. Plamondon, A. Marcelli, and M.A. Ferrer (Eds.), The Lognormality Principle and its Applications, World Scientific*, 2019.

[12] M.A. Ferrer, M. Diaz, C.A. Carmona, and R. Plamondon, “iDeLog: Iterative Dual Spatial and Kinematic Extraction of Sigma-Lognormal Parameters,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2018.

[13] 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, 2015.

[14] R. Tolosana, R. Vera-Rodriguez, and J. Fierrez, “BioTouchPass: Handwritten Passwords for Touchscreen Biometrics,” *IEEE Transactions on Mobile Computing*, 2019.

[15] M. Harbach, A. D. Luca, and S. Egelman, “The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens,” in *Proc. Conference on Human Factors in Computing Systems*, 2016, pp. 4806–4817.

[16] A. Acien, A. Morales, J. Fierrez, R. Vera-Rodriguez, and J. Hernandez-Ortega, “Active Detection of Age Groups Based on Touch Interaction,” *IET Biometrics*, vol. 8, pp. 101–108, 2019.

[17] R. Vera-Rodriguez, R. Tolosana, M. Caruana, G. Manzano, C. Gonzalez-Garcia, J. Fierrez and J. Ortega-Garcia, “DeepSignCX: Signature Complexity Detection using Recurrent Neural Networks,” in *Proc. International Conference on Document Analysis and Recognition*, 2019.

[18] S. Otte, M. Liwicki and D. Krechel, “Investigating Long Short-Term Memory Networks for Various Pattern Recognition Problems,” *Machine Learning and Data Mining in Pattern Recognition*, Springer, 2014.

[19] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, “Exploring Recurrent Neural Networks for On-Line Handwritten Signature Biometrics,” *IEEE Access*, vol. 6, pp. 5128–5138, 2018.

[20] S. Lai and L. Jin, “Recurrent Adaptation Networks for Online Signature Verification,” *IEEE Transactions on Information Forensics and Security*, pp. 1–14, 2018.

[21] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J. Ortega-Garcia, “Presentation Attacks in Signature Biometrics: Types and Introduction to Attack Detection,” *S. Marcel, M.S. Nixon, J. Fierrez and N. Evans (Eds.), Handbook of Biometric Anti-Spoofing (2nd Edition), Springer*, 2019.

[22] J. Ortega-Garcia, J. Fierrez-Aguilar, and *et al.*, “MCYT Baseline Corpus: A Bimodal Biometric Database,” *Proc. IEEE Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet*, vol. 150, no. 6, pp. 395–401, 2003.

[23] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. Freire, F. Alonso-Fernandez, D. Ramos, D. Toledano, J. Gonzalez-Rodriguez, J. Siguenza, J. Garrido-Salas *et al.*, “BiosecurID: A Multimodal Biometric Database,” *Pattern Analysis and Applications*, vol. 13, no. 2, pp. 235–246, 2010.

[24] J. Ortega-Garcia, J. Fierrez, and *et al.*, “The Multi-Scenario Multi-Environment BioSecure Multimodal Database (BMDB),” *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 32, no. 6, pp. 1097–1111, 2010.

[25] M. Salehan and A. Negahban, “Social Networking on Smartphones: When Mobile Phones Become Addictive,” *Computers in Human Behavior*, vol. 29, no. 6, pp. 2632–2639, 2013.

[26] S. Pan and Q. Yang, “A Survey on Transfer Learning,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 22, no. 10, pp. 1345–1359, 2010.

[27] J. Hu, J. Lu, and Y. Tan, “Deep Transfer Metric Learning,” in *Proc. Conf. on Computer Vision and Pattern Recognition*, 2015, pp. 325–333.