Chapter 16
Introduction to Presentation Attacks in Signature Biometrics and Recent Advances

Carlos Gonzalez-Garcia, Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia

Abstract Applications based on biometric authentication have received a lot of interest in the last years due to the breathtaking results obtained using personal traits such as face or fingerprint. However, it is important not to forget that these biometric systems have to withstand different types of possible attacks. This chapter carries out an analysis of different Presentation Attack (PA) scenarios for on-line handwritten signature verification. The main contributions of this chapter are: *(i)* an updated overview of representative methods for Presentation Attack Detection (PAD) in signature biometrics; *(ii)* a description of the different levels of PAs existing in on-line signature verification regarding the amount of information available to the impostor, as well as the training, effort, and ability to perform the forgeries; and *(iii)* an evaluation of the system performance in signature biometrics under different scenarios considering recent publicly available signature databases, DeepSignDB (https://github.com/BiDAlab/DeepSignDB) and SVC2021_EvalDB (https://github.com/BiDAlab/SVC2021_EvalDB), (https://competitions.codalab.org/competitions/27295). This work is in line with recent efforts in the Common Criteria standardization community towards security evaluation of biometric systems.

C. Gonzalez-Garcia · R. Tolosana (✉) · R. Vera-Rodriguez (✉) · J. Fierrez (✉) · J. Ortega-Garcia
Biometrics and Data Pattern Analytics—BiDA Lab, Escuela Politecnica Superior, Universidad Autonoma de Madrid, 28049 Madrid, Spain
e-mail: ruben.tolosana@uam.es

R. Vera-Rodriguez
e-mail: ruben.vera@uam.es

J. Fierrez
e-mail: julian.fierrez@uam.es

C. Gonzalez-Garcia
e-mail: carlos.gonzalezgarcia@estudiante.uam.es

J. Ortega-Garcia
e-mail: javier.ortega@uam.es

S. Marcel et al. (eds.), *Handbook of Biometric Anti-Spoofing*, Advances in Computer Vision and Pattern Recognition, https://doi.org/10.1007/978-981-19-5288-3_16

16.1 Introduction

Signature verification systems have become very popular in many applications such as banking, e-health, e-education, and security in recent times [1]. This evolution has been motivated due to two main factors: (*i*) the technological evolution and the improvement of sensors quality, which has made general purpose devices (smartphones [2] and tablets [3]) more accessible to the general population, and therefore, the social acceptance has increased; and (*ii*) the evolution of biometric recognition technologies, especially through the use of deep learning techniques [4, 5]. However, it is important to highlight that this biometric systems have to endure different types of possible attacks [6, 7], some of them highly complex [8].

In this chapter we focus on the study of different Presentation Attack (PA) scenarios for on-line handwritten signature biometric verification systems due to the significant amount of attention received in the last years thanks to the development of new scenarios (e.g. device interoperability [9] and mobile scenarios [10, 11]) and writing tools (e.g. finger [2]). These new scenarios have grown hand in hand with the rapid expansion of mobile devices, such as smartphones, which allow the implementation of biometric-based verification systems far from the traditional office-like ones [12].

In general, two different types of impostors can be found in the context of signature verification: (1) *random (zero-effort* or *accidental)* impostors, the case in which no information about the signature of the user being attacked is known and impostors present their own genuine signature claiming to be another user of the system, and (2) *skilled* impostors, the case in which attackers have some level of information about the signature of the user to attack (e.g. global shape of the signature or signature dynamics) and try to forge the signature claiming to be that user in the system.

In [13], Galbally et al. discussed different approaches to report accuracy results in handwritten signature verification. They considered skilled impostors as a particular case of biometric PAs which is performed against a behavioural biometric characteristic (also referred as *mimicry*). There are important differences between PAs and mimicry: while traditional PAs involve the use of some physical artefacts such as fake masks and gummy fingers (and therefore, they can be detected in some cases at the sensor level), in the case of mimicry the interaction with the sensor is exactly the same followed in a genuine access attempt. In [13] a different nomenclature of impostor scenarios is proposed following the literature standard in the field of biometric Presentation Attack Detection (PAD) : the classical random impostor scenario is referred to as Bona Fide (BF) scenario, while the skilled impostor scenario is referred to as PA scenario. This nomenclature has also been used in this chapter.

If during the development of a biometric verification system those PAs are expected, it is possible to include specific modules for PAD, which in the signature verification literature are commonly referred to as forgery detection modules. A comprehensive study of these PAD methods is out of the scope of the chapter, but in Sect. 16.2 we provide a brief overview of some selected representative works in that area.

A different approach to improve the security of a signature verification system against attacks different from including a PAD module is template protection [14–20]. Traditional on-line signature verification systems work with very sensitive biometric data such as the X and Y spatial coordinates and store that information without any additional protection. This makes very easy for attackers to steal this information. If an attacker has the information of spatial coordinates along the time axis it would be very easy for him/her to generate very high quality forgeries. Template protection techniques involve feature transformation and the use of biometric cryptosystems. In [21], an extreme approach for signature template generation was proposed not considering information related to X, Y coordinates and their derivatives on the biometric system, providing therefore a much more robust system against attacks, as this critical information would not be stored anywhere. Moreover, the results achieved had error rates in the same range as more traditional systems which store very sensitive information. An interesting review and classification of different biometric template protection techniques for on-line handwritten signature application is conducted in [22].

The main contributions of this chapter are: *(i)* a brief overview of representative methods for PAD in signature biometrics ; *(ii)* a description of the different levels of PAs existing in on-line signature verification regarding the amount of information available to the impostor, as well as the training, effort and ability to perform the forgeries; and *(iii)* an evaluation of the system performance in signature biometrics under different scenarios following the recent SVC-onGoing competition[1] [23].

The remainder of the chapter is organized as follows. The introduction is completed with a short overview of PAD in signature biometrics (Sect. 16.2). After that, the main technical content of the chapter begins in Sect. 16.3, with a review of the most relevant features of all different impostor scenarios, pointing out which type of impostors are included in many different well-known public signature databases. Section 16.4 describes the on-line signature databases considered in the experimental work. Section 16.5 describes the experimental protocol and the results achieved. Finally, Sect. 16.6 draws the final conclusions and points out some lines for future work.

16.2 Review of PAD in Signature Biometrics

Presentation Attack Detection (PAD) in signature biometrics is a field that has been extensively studied since the late 70s to the present [24]. In this section we describe some state-of-the-art forgery detection methods.

Some of the studies that can be found in the literature are based on the *Kinematic Theory* of rapid human movements and its associated Sigma LogNormal model. In [25], the authors proposed a new scheme in which a module focused on the detection

[1] https://competitions.codalab.org/competitions/27295.

of skilled forgeries (i.e. PA impostors) was based on four parameters of the Sigma LogNormal writing generation model [26] and a linear classifier. That new binary classification module was supposed to work sequentially before a standard signature recognition system [27]. Good results were achieved using that approach for both skilled (i.e. PA) and random (i.e. BF) scenarios. In [28], Reillo et al. proposed PAD methods based on the use of some global features such as the total number of strokes and the signing time of the signatures. They acquired a new database based on 11 levels of PAs regarding the level of knowledge and the tools available to the forger. The results achieved in that work using the proposed PAD methods reduced the Equal Error Rate (EER) from a percentage close to 20.0% to below 3.0%.

In [29], authors proposed an off-line signature verification and forgery detection system based on fuzzy modelling. The verification of genuine signatures and detection of forgeries was achieved via angle features extracted using a grid method. The derived features were fuzzified by an exponential membership function, which was modified to include two structural parameters regarding variations of the handwriting styles and other factors affecting the scripting of a signature. Experiments showed the capability of the system in detecting even the slightest changes in signatures.

Brault and Plamondon presented in [30] an original attempt to estimate, quantitatively and a priori from the coordinates sampled during its execution, the difficulty that could be experienced by a typical imitator in reproducing both visually and dynamically that signature. To achieve this goal, they first derived a functional model of what a typical imitator must do to copy dynamically any signature. A specific difficulty coefficient was then numerically estimated for a given signature. Experimentation geared specifically to signature imitation demonstrated the effectiveness of the model. The ranking of the tested signatures given by the difficulty coefficient was compared to three different sources: the opinions of the imitators themselves, the ones of an expert document examiner, and the ranking given by a specific pattern recognition algorithm. They provided an example of application as well. This work was one of the first attempts of PAD for on-line handwritten signature verification using a special pen attached to a digitizer (Summagraphic Inc. model MM1201). The sampling frequency was 110 Hz, and the spatial resolution was 0.025 in.

Finally, it is important to highlight that new approaches based on deep learning architectures are commonly used in the literature [5, 23]. Several studies use Convolutional Neural Network (CNN) architectures in order to predict whether a signature is genuine or a forgery presented by a PA impostor [31–33]. Other state-of-the-art architectures are based on Recurrent Neural Networks (RNNs) such as the ones presented in [34]. Also, some recent works focus on analyzing the system performance against both BF and PA scenarios depending of the signature complexity [35, 36].

16.3 Presentation Attacks in Signature Biometrics

The purpose of this section is to clarify the different levels of skilled forgeries (i.e. PA impostors) that can be found in the signature biometrics literature regarding the amount of information provided to the attacker, as well as the training, effort and ability to perform the forgeries. In addition, the case of random forgeries (i.e. zero-effort impostors) is also considered although it belongs to the BF scenario and not to the PA scenario in order to review the whole range of possible attacks in on-line signature verification.

Previous studies have applied the concept of Biometric Menagerie in order to categorize each type of user of the biometric system as an animal. This concept was initially formalized by Doddington et al. in [37], classifying speakers regarding the ease or difficulty with which the speaker can be recognized (i.e. sheep and goats, respectively), how easily they can be forged (i.e. lambs) and finally, how adept/effective they are at forging/imitating the voice of others (i.e. wolves). Yager and Dunstone extended the Biometric Menagerie in [38] by adding four more categories of users (i.e. worms, chameleons, phantoms, and doves). Their proposed approach was investigated using a broad range of biometric modalities, including 2D and 3D faces, fingerprints, iris, speech, and keystroke dynamics. In [39], Houmani and Garcia-Salicetti applied the concept of Biometric Menagerie for the different types of users found in the on-line signature verification task proposing the combination of their personal and relative entropy measures as a way to quantify how difficult it is a signature to be forged. Their proposed approach achieved promising classification results on the MCYT database [40], where the attacker had access to a visual static image of the signature to forge.

In [41], some experiments were carried out to reach the following conclusions: (1) some users are significantly better forgers than others; (2) forgers can be trained in a relatively straight-forward way to become a greater threat; (3) certain users are easy targets for forgers; and (4) most humans are relatively poor judges of handwriting authenticity, and hence, their unaided instincts cannot be trusted. Additionally, in that work authors proposed a new metric for impostor classification more realistic to the definition of security, i.e., *naive*, *trained*, and *generative*. They considered naive impostors as random impostors (i.e. zero-effort impostors) in which no information about the user to forge is available whereas they referred to trained and generative impostors to skilled forgeries (i.e. PA impostors) when only the image or the dynamics of the signature to forge is available, respectively.

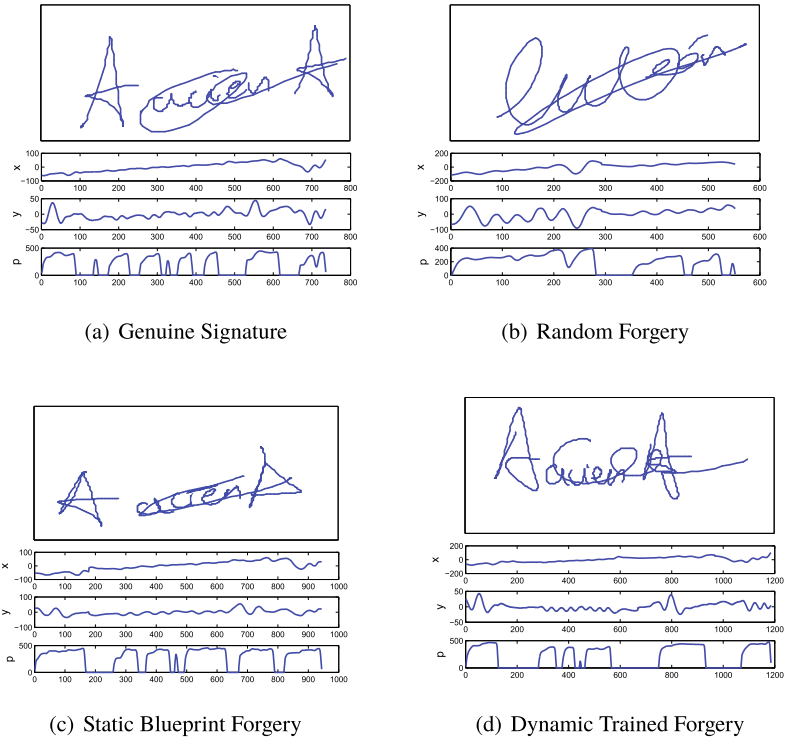
In [42], the authors proposed a software tool implemented on two different computer platforms in order to achieve forgeries with different quality levels (i.e. PA impostors). Three different levels of PAs were considered: (1) *blind forgeries*, the case in which the attacker writes on a blank surface having access just to textual knowledge (i.e. precise spelling of the user's name to forge); (2) *low-force forgeries*, where the attacker gets a blueprint of the signature projected on the writing surface (dynamic information is not provided), which they may trace; and (3) *brute-force forgeries*, in which an animated pointer is projected onto the writing pad showing the

whole realization of the signature to forge. The attacker may observe the sequence and follow the pointer. The authors carried out an experiment based on the use of 82 forgery samples performed by four different users in order to detect how the False Acceptance Rate (FAR) is affected regarding the level of PA. They considered a signature verification system based on the average quadratic deviation horizontal and vertical writing signals. Results obtained for four different threshold values confirmed the requirement of strong protection of biometric reference data as it was proposed in [21].

16.3.1 Types of Presentation Attacks

Alonso-Fernandez et al. carried out an exhaustive analysis of the different types of forgeries found in handwritten signature verification systems [43]. In that work, authors considered random impostors and 4 different levels of PA impostors, classified regarding the amount of information provided and the tools used by the attacker in order to forge the signature:

- **Random or zero-effort forgeries**, in which no information of the user to forge is available and the attacker uses its own genuine signature (accidentally or not) claiming to be another user of the system.
- **Blind forgeries**, in which the impostor has access to a descriptive or textual knowledge of signatures to forge (e.g. the name of the subject to forge).
- **Static forgeries** (low-force in [42]), where the attacker has available a static image of the global shape of the signature to forge. In this case, there are two ways to generate the forgeries. In the first one, the attacker can train to imitate the signature with or without time restrictions and blueprint, and then forge it without the use of the blueprint, which leads to **static trained forgeries**. In the second one, the attacker uses a blueprint to first copy the genuine signature of the user to forge and then put it on the screen of the device while forging, leading to **static blueprint forgeries**, more difficult to detect as they have quite the same appearance as the original ones.
- **Dynamic forgeries** (brute-force in [42]), where the impostor has access to both the global image and also the whole realization process (i.e. dynamics) of the signature to forge. The dynamics can be obtained in the presence of the original writer or through the use of a video-recording. In a similar way as the previous category, we can distinguish first **dynamic trained forgeries** in which the attacker can use specific tools to analyze and train to forge the genuine signature, and second, **dynamic blueprint forgeries** which are generated by projecting on the acquisition area a real-time pointer that the forger only needs to follow.
- **Regained forgeries**, the case where the impostor has only available the static image of the signature to forge and makes use of a dedicated software to recover the signature dynamics [44], which are later analyzed and used to create dynamic forgeries.



(a) Genuine Signature (b) Random Forgery

(c) Static Blueprint Forgery (d) Dynamic Trained Forgery

Fig. 16.1 Examples of one genuine signature and three different types of forgeries performed for the same user

As expected, dynamic forgeries are the forgeries with better quality (in some cases, very similar to the genuine signatures that are forged), followed by static forgeries. Random and blind forgeries are usually very different from the signature forged. Figure 16.1 shows examples of a genuine signature and three different types of forgeries (i.e. random, static blueprint and dynamic trained) performed for the same user. The image shows both the static and dynamic information with the X and Y coordinates and pressure.

Besides the forgery classification carried out in [43], Alonso-Fernandez et al. studied the impact of an incremental level of quality forgeries against handwritten signature verification systems. The authors considered off-line and on-line systems using the BiosecurID database [45]. For the off-line verification system, they considered a system based on global image analysis and a minimum distance classifier [46] whereas a system based on Hidden Markov Models (HMM) [47] was considered for the on-line system. The experiments carried out proved that the performance of the off-line approach is only degraded when the highest quality level of forgeries is used. The on-line system shows a progressive degradation of its performance when the quality level of the forgeries is increased. This lead the authors to the conclusion

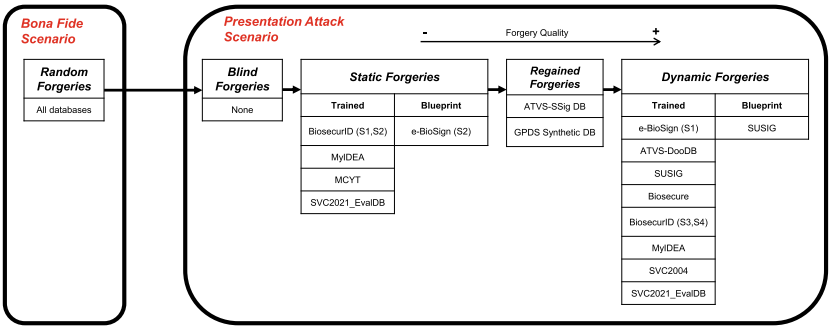


Fig. 16.2 Diagram of different types of forgeries for both BF and PA scenarios regarding the amount of information provided to the attacker, as well as the training, effort, and ability to perform them. The most commonly used on-line signature databases are included to each PA group

that the dynamic information of signatures is the one more affected when the quality of the forgeries increases.

Finally, Fig. 16.2 summarizes all different types of forgeries for both BF and PA scenarios regarding the amount of information provided to the impostor, as well as the training, effort, and ability to perform them. In addition, the most commonly used on-line signature databases are included to each PA group in order to provide an easy representation. To the authors' best knowledge, there are no publicly available on-line signature databases for the case of blind forgeries.

16.3.2 Synthetic Forgeries

On-line signature synthesis has become a very interesting research line due to, among other reasons, the lack of forgery signatures in real scenarios, which makes the development of robust signature verification systems difficult [4].

One of the most popular approaches in the literature for realistic handwriting generation was presented in [48]. In that study, the author presented a Long Short-Term Memory (LSTM) Recurrent Neural Network (RNN) architecture to generate complex sequences. The proposed architecture was tested on handwriting, achieving very good visual results. Currently, the Sigma LogNormal model is one of the most popular on-line signature synthesis approaches [49, 50], and has been applied to on-line signature verification systems, generating synthetic samples from a genuine signature, increasing the amount of information and improving the performance of the systems [51–53].

Other important contributions in this area are the following ones. In [44], Ferrer et al. proposed a system for the synthetic generation of dynamic information for both static and dynamic handwritten signatures based on the motor equivalence theory, which divides the action of human handwriting into an effector dependent

cognitive level and an effector independent motor level, achieving good results. In [54], Tolosana et al. proposed DeepWriteSYN, a novel on-line handwriting signature synthesis approach based on deep short-term representations. The DeepWriteSYN architecture is composed by two modules: a first module which divides the signature in short-time strokes and a second module based on a sequence-to-sequence Variational Autoencoder (VAE) in charge of the synthesis of those short-time strokes. DeepWriteSYN is able to generate realistic handwriting variations of a given handwritten structure corresponding to the natural variation within a given population or a given subject. For more information, an exhaustive study of the evolution of synthetic handwriting is conducted in [55].

16.4 On-Line Signature Databases

The following two public databases are considered in the experiments reported here. Both of them are currently used in the popular SVC-onGoing on-line signature verification competition.[2]

16.4.1 DeepSignDB

The DeepSignDB[3] database [56] is composed by a total of 1,526 subjects from four different well known state-of-the-art databases: MCYT (330 subjects) [40], BiosecurID (400 subjects) [45], Biosecure DS2 (650 subjects) [57], e-BioSign (65 subjects) [2], and a novel on-line signature database composed by 81 subjects. DeepSignDB comprises more than 70 K signatures acquired using both stylus and finger writing inputs in both office and mobile scenarios. A total of 8 different devices were considered during the acquisition process (i.e., 5 Wacom devices and 3 Samsung general purpose devices). In addition, different types of impostors and number of acquisition sessions are considered along the database.

The available information when using the pen stylus as writing input is X and Y spatial coordinates and pressure. In addition, pen-up trajectories are also available. For the case of using the finger as writing input, the only available information is X and Y spatial coordinates.

[2] https://competitions.codalab.org/competitions/27295.

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

16.4.2 SVC2021_EvalDB

The SVC2021_EvalDB[4] is a novel database specifically acquired for the ICDAR 2021 Signature Verification Competition [23] and then used as well for the SVC-onGoing Competition [23]. In this database, two scenarios are considered: office and mobile scenarios.

- **Office scenario:** on-line signatures from 75 subjects were collected using a Wacom STU-530 device with the stylus as writing input. It is important to highlight that all the acquisition took place in an office scenario under the supervision of a person with experience in the on-line signature verification field. The subjects considered in the acquisition of SVC2021_EvalDB database are different compared to the ones considered in the previous DeepSign database. All the signatures were collected in two different sessions separated by at least 1 week. For each genuine subject, a total of 8 genuine signatures (4 genuine signatures per session) and 16 skilled forgeries (8 static forgeries and 8 dynamic forgeries, performed by 4 different subjects in two different sessions) were collected. Regarding the skilled forgeries, static forgeries were collected in the first acquisition session and dynamic forgeries were considered in the second one. The following information is available for every signature: X and Y spatial coordinates, pressure, pen-up trajectories and timestamp.
- **Mobile scenario:** on-line signatures from a total of 119 subjects were acquired using the same acquisition framework considered in MobileTouchDB database [12]: an Android App was developed in order to work with unsupervised mobile scenarios. All users could download the application and use it on their own smartphones without any kind of supervision, simulating a real scenario (e.g., standing, sitting, walking, in public transport, etc.). As a result, a total of 94 different smartphone models from 16 different brands are available in the database. Regarding the acquisition protocol, between four and six separated sessions were acquired for every user with a time gap between first and last session of at least 3 weeks. The number and type of the signatures for every user is the same as on the office scenario. Timestamp and spatial coordinates X and Y are available for every signature.

16.5 Experimental Work

16.5.1 On-line Signature Verification System

We consider for the experimental analysis the state-of-the-art signature verification system presented in [5, 12] based on Time-Alignment Recurrent Neural Network (TA-RNN).

[4] https://github.com/BiDAlab/SVC2021_EvalDB.

For the input of the system, the network is fed with 23 time functions extracted from the signature [58]. Information related to the azimuth and altitude of the pen angular orientation is not considered in this case. The TA-RNN architecture is based on two consecutive stages: *(i)* time sequence alignment through DTW (*Dynamic Time Warping*) , and *(ii)* feature extraction and matching using a RNN. The RNN system comprises three layers. The first layer is composed of two Bidirectional Gated Recurrent Unit (BGRU) hidden layers with 46 memory blocks each, sharing the weights between them. The outputs of the first two parallel BGRU hidden layers are concatenated and serve as input to the second layer, which corresponds to a BGRU hidden layer with 23 memory blocks. Finally, a feed-forward neural network layer with a sigmoid activation is considered, providing an output score for each pair of signatures. This learning model was presented in [5] and was retrained for the SVC-onGoing competition [23] adapted to the stylus scenario by using only the stylus-written signatures of the development set of DeepSignDB (1,084 users). The best model has been then selected using a partition of the development set of DeepSignDB, leaving out of the training the DeepSignDB evaluation set (442 users).

16.5.2 Experimental Protocol

The experimental protocol has been designed to allow the study of both random forgeries (i.e. BF) and skilled forgeries (i.e. PA) scenarios on the system performance. Additionally, the case of using the stylus or the finger as writing tool is considered.

For the study of the writing input impact in the system performance, the same three scenarios considered in the SVC-onGoing competition [23] have been used:

- **Task 1:** analysis of office scenarios using the stylus as input.
- **Task 2:** analysis of mobile scenarios using the finger as input.
- **Task 3:** analysis of both office and mobile scenarios simultaneously.

For the development of the system, the training dataset of the DeepSignDB database (1084 subjects) has been used. This means that the system has been trained using only signatures captured with a stylus writing tool. This will have a considerable impact on the system performance, as will be seen in Sect. 16.5.3. It is also important to highlight that, in order to consider a very challenging impostor scenario, the skilled forgery comparisons included in the evaluation datasets (not in the training ones) of both databases have been optimised using machine learning methods, selecting only the best high-quality forgeries.

In addition, SVC-onGoing simulates realistic operational conditions **considering random and skilled forgeries simultaneously in each task.** A brief summary of the proposed experimental protocol used can be seen in Fig. 16.3. For more details, we refer the reader to [23].

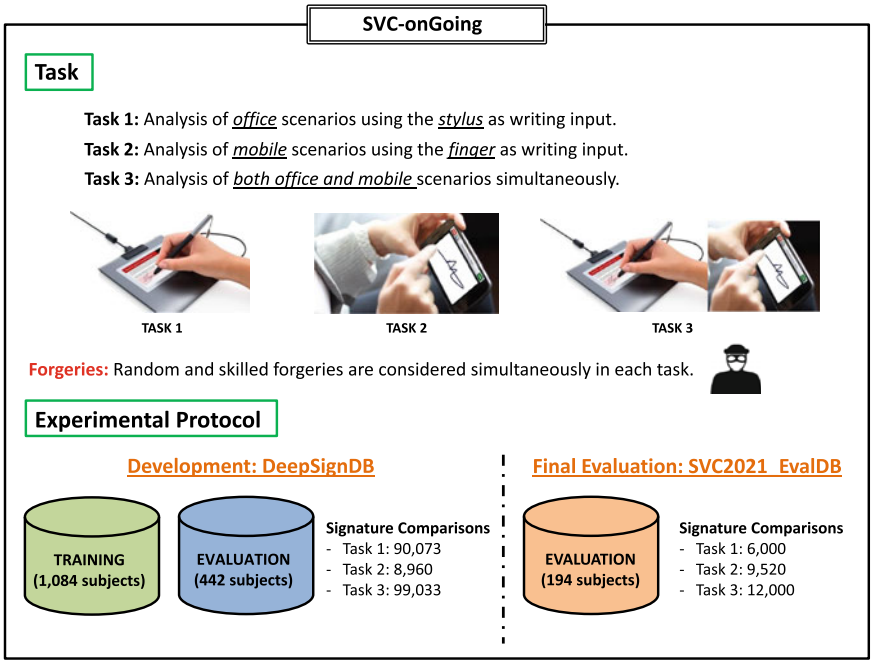


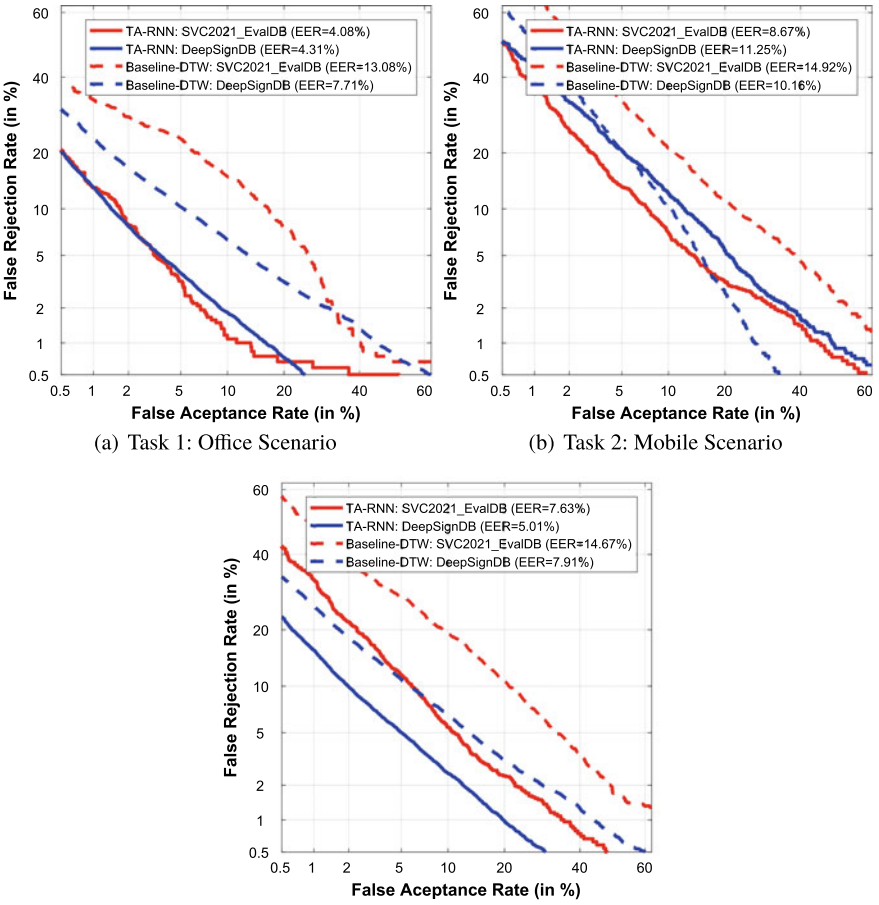
Fig. 16.3 Description of the tasks and experimental protocol details considered in SVC-onGoing Competition

16.5.3 Experimental Results

This section analyzes the results achieved in both DeepSignDB and SVC2021_EvalDB databases.

16.5.3.1 DeepSignDB

In this first case, the evaluation dataset (442 subjects) of DeepSignDB was used to evaluate the performance of both DTW and TA-RNN systems. Figure 16.4 shows the results achieved in each of the three tasks using Detection Error Tradeoff (DET) curves and considering both random and skilled forgeries simultaneously. A Baseline DTW system (similar to the one described in [59] based on X, Y spatial time signals, and their first- and second-order derivatives) is included in the image for a better comparison of the results. First, in all tasks we can see that the TA-RNN system has outperformed the traditional Baseline DTW. For Task 1, focused on the analysis of office scenarios using the stylus as writing input, the TA-RNN approach obtained a 4.31% EER. Regarding Task 2, focused on mobile scenarios using the finger as writing input, a considerable system performance degradation is observed compared



(a) Task 1: Office Scenario

(b) Task 2: Mobile Scenario

(c) Task 3: Office/Mobile Scenario

Fig. 16.4 Task Analysis: Results in terms of DET curves over the evaluation dataset of DeepSignDB and SVC2021_EvalDB for the three tasks considered

to the results of Task 1. In this case, the EER obtained was 11.25%. This result proves the bad generalisation of the stylus model (Task 1) to the finger scenario (Task 2) as the model considered was trained using only signatures acquired through the stylus, not the finger. Finally, good results are generally achieved in Task 3 taking into account that both office and mobile scenarios are considered together, using both stylus and finger as writing inputs. The system obtained an EER of 5.01%.

16.5.3.2 SVC2021_EvalDB

In this section we present the results obtained in the evaluation of the novel *SVC2021_EvalDB* database. Similar to the previous section, we include in Fig. 16.4 the Baseline DTW system.

It is important to highlight that TA-RNN achieves good EER results in the three tasks (4.08%, 8.67% and 7.63% respectively) even if it is only trained with signatures introduced using the stylus as writing input. Also, it is interesting to compare the results achieved in each task with the results obtained using traditional approaches in the field (Baseline DTW). Concretely, for each of the tasks, the TA-RNN architecture achieves relative improvements of 68.81, 41.89, and 47.99% EER compared to the Baseline DTW. These results prove the high potential of deep learning approaches such as TA-RNN for the on-line signature verification field, as commented in previous studies [5, 33, 54].

Another key aspect to analyse is the generalisation ability of the proposed system against new users and acquisition conditions (e.g., new devices). This analysis is possible as different databases are considered in the development and final evaluation of the competition. Figure 16.4 show the results achieved using the DeepSignDB and SVC2021_EvalDB databases, respectively. For Task 1, we can observe the good generalisation ability of the TA-RNN system, achieving results of 4.31% EER for the development, and 4.08% EER for the evaluation. Regarding Task 2, it is interesting to highlight that the TA-RNN system also obtains reasonable generalisation results. Similar trends are observed in Task 3.

Finally, for completeness, we also analyse the False Acceptance Rate (FAR) and False Rejection Rate (FRR) results of the proposed systems. Looking at Fig. 16.4, in general, for low values of FAR (i.e., high security), the TA-RNN system achieves good results in all tasks. It is interesting to remark that depending on the specific task, the FRR values for low values of FAR are very different. For example, analysing a FAR value of 0.5%, the FRR value is around 20% for Task 1. However, the FRR value increases over 40% for Task 2, showing the challenging conditions considered in real mobile scenarios using the finger as writing input. A similar trend is observed for low values of FRR (i.e., high convenience).

16.5.3.3 Forgery Analysis

This section analyzes the impact of the type of forgery in the proposed on-line signature verification system. In the evaluation of SVC-onGoing, both random and skilled forgeries are considered simultaneously in order to simulate real scenarios. Therefore, the winner of the competition was the system that achieved the highest robustness against both types of impostors at the same time [23]. We now analyse the level of security of the two systems considered for each type of forgery, i.e., random and skilled. Figure 16.5 shows the DET curves of each task and type of forgery, including also the EER results, over both DeepSignDB and SVC2021_EvalDB databases.

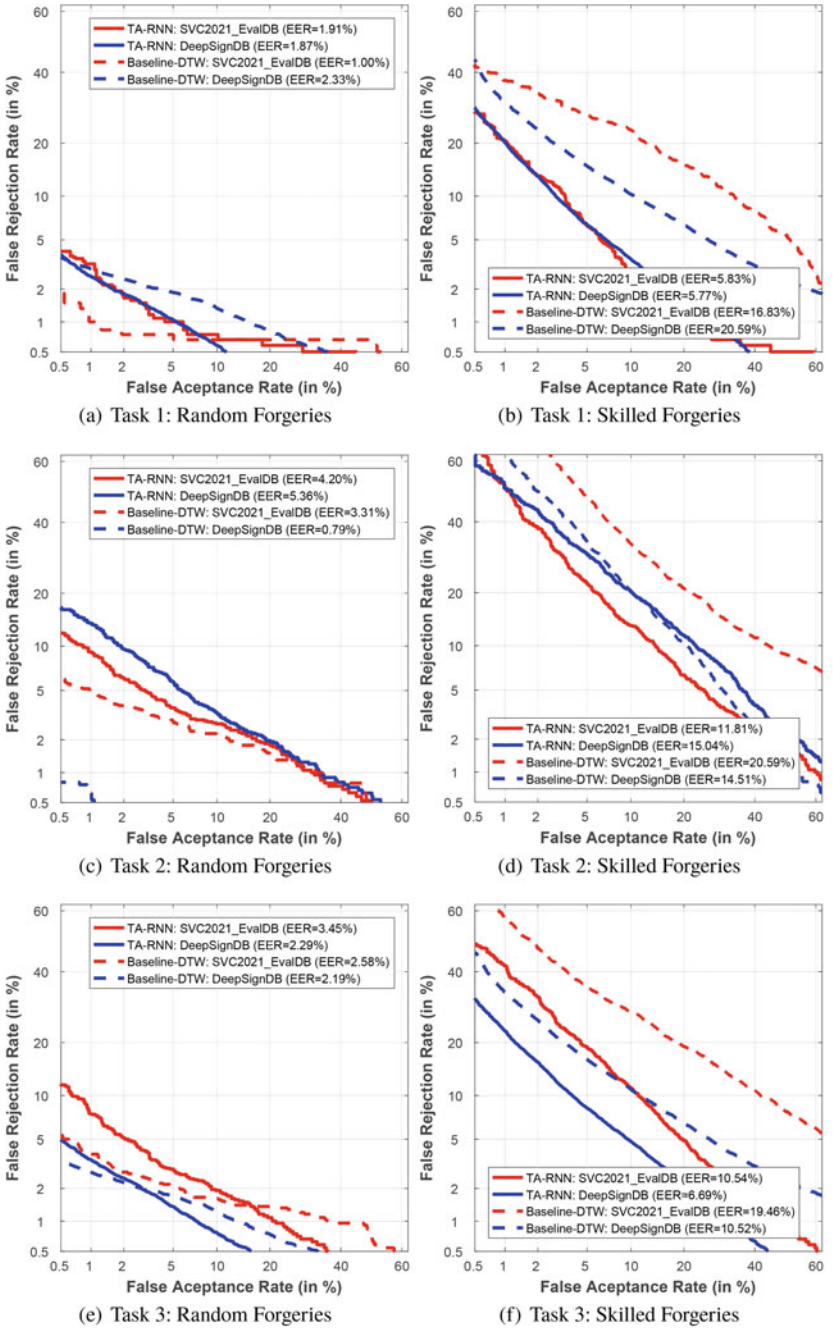


Fig. 16.5 Forgery Analysis: Results in terms of DET curves over the evaluation dataset of DeepSignDB and SVC2021_EvalDB for the three tasks and both types of forgeries separately

Analysing the skilled forgery scenario (Fig. 16.5b, d, and f), in all cases the TA-RNN system achieves the best results in terms of EER, outperforming the traditional Baseline DTW system in both SVC2021_EvalDB and DeepSignDB databases.

Regarding the random forgery scenario, interesting results are observed in Fig. 16.5a, c, and e. In general, the TA-RNN system obtains worse results in terms of EER compared to the Baseline DTW system, which obtains EER results of 1.00, 3.31, and 2.58% (SVC2021_EvalDB) and 2.33, 0.79 and 2.19% (DeepSignDB) for each of the corresponding tasks of the competition, proving the potential of DTW for the detection of random forgeries. A similar trend was already discovered in previous studies in the literature [34], highlighting also the difficulties of deep learning models to detect both skilled and random forgeries simultaneously.

Finally, seeing the results included in Fig. 16.5, we also want to highlight the very challenging conditions considered in SVC-onGoing compared with previous international competitions. This is produced mainly due to the real scenarios studied in the competition, e.g., several acquisition devices and types of impostors, large number of subjects, etc.

16.6 Conclusions

This chapter carries out an analysis of Presentation Attack (PA) scenarios for on-line handwritten signature verification. Unlike traditional PAs, which use physical artefacts (e.g. gummy fingers and fake masks), the most typical PAs in signature verification represent an impostor interacting with the sensor in a very similar way followed in a normal access attempt (i.e., the PA is a handwritten signature, in this case trying to imitate to some extent the attacked identity). In a typical signature verification PA scenario, the level of knowledge that the impostor has and uses about the signature being attacked, as well as the effort and the ability to perform the forgeries, results crucial for the success rate of the system attack.

The main contributions of this chapter are: (1) a brief overview of representative methods for PAD in signature biometrics; (2) the description of the different levels of PAs existing in on-line signature verification regarding the amount of information available to the impostor, as well as the training, effort and ability to perform the forgeries; and (3) analysis of system performance evaluation in signature biometrics under different PAs and writing tools considering new and publicly available signature databases.

Results obtained for both DeepSignDB and SVC2021_EvalDB publicly available databases show the high impact on the system performance regarding not only the level of information that the attacker has but also the training and effort performing the signature. For the case of users using the finger as the writing tool, a recommendation for the usage of signature verification on smartphones on mobile scenarios (i.e., sitting, standing, walking, indoors, outdoors, etc.) would be to protect themselves from other people that could be watching while performing their genuine signature, as this is more feasible to do in a mobile scenario compared to an office scenario.

This way skilled impostors (i.e. PA impostors) might have access to the global image of the signature but not to the dynamic information and system performance would be much better. This work is in line with recent efforts in the Common Criteria standardization community towards security evaluation of biometric systems, where attacks are rated depending on, among other factors: time spent, effort, and expertise of the attacker; as well as the information available and used from the target being attacked [60].

Acknowledgements The chapter update for the 3rd Edition of the book has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 860315 (PRIMA) and No 860813 (TRESPASS-ETN). Partial funding also from INTER-ACTION (PID2021-126521OB-I00 MICINN/FEDER), Orange Labs, and Cecabank.

References

1. Faundez-Zanuy M, Fierrez J, Ferrer MA, Diaz M, Tolosana R, Plamondon R (2020) Handwriting biometrics: applications and future trends in e-security and e-health. Cogn Comput 12(5):940–953
2. Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J (2017) Benchmarking desktop and mobile handwriting across COTS devices: the e-BioSign biometric database. PLOS ONE 1–17
3. Alonso-Fernandez F, Fierrez-Aguilar J, Ortega-Garcia J (2005) Sensor interoperability and fusion in signature verification: a case study using tablet PC. In: Proceedings of the IWBRS, LNCS, vol 3781. Springer, pp 180–187
4. Diaz M, Ferrer MA, Impedovo D, Malik MI, Pirlo G, Plamondon R (2019) A perspective analysis of handwritten signature technology. ACM Comput Surv (Csur) 51(6):1–39
5. Tolosana R, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J (2021) DeepSign: deep on-line signature verification. IEEE Trans Biom Behav Ident Sci
6. Galbally J, Fierrez J, Ortega-Garcia J (2007) Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. In: Proceedings of the Spanish workshop on biometrics, (SWB)
7. Rathgeb C, Tolosana R, Vera-Rodriguez R, Busch C (2021) Handbook of digital face manipulation and detection: from DeepFakes to morphing attacks. Advances in computer vision and pattern recognition. Springer
8. Hadid A, Evans N, Marcel S, Fierrez J (2015) Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Process Mag 32(5):20–30. https://doi.org/10.1109/MSP.2015.2437652
9. Tolosana R, Vera-Rodriguez R, Ortega-Garcia J, Fierrez J (2015) Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification. IEEE Access 3:478–489
10. Impedovo D, Pirlo G (2021) Automatic signature verification in the mobile cloud scenario: survey and way ahead. IEEE Trans Emerg Top Comput 9(1):554–568
11. Martinez-Diaz M, Fierrez J, Galbally J, Ortega-Garcia J (2009) Towards mobile authentication using dynamic signature verification: useful features and performance evaluation, pp 1 – 5
12. Tolosana R, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J (2020) BioTouchPass2: touchscreen password biometrics using time-aligned recurrent neural networks. IEEE Trans Inf Forensics Secur 5:2616–2628

13. Galbally J, Gomez-Barrero M, Ross A (2017) Accuracy evaluation of handwritten signature verification: rethinking the random-skilled forgeries dichotomy. In: Proceedings of the IEEE international joint conference on biometrics, pp 302–310
14. Campisi P, Maiorana E, Fierrez J, Ortega-Garcia J, Neri A (2010) Cancelable templates for sequence based biometrics with application to on-line signature recognition. IEEE Trans Syst Man Cybernet Part A: Syst Humans 3:525–538
15. Delgado-Mohatar O, Fierrez J, Tolosana R, Vera-Rodriguez R (2019) Biometric template storage with blockchain: a first look into cost and performance tradeoffs. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops
16. Freire MR, Fierrez J, Ortega-Garcia J (2008) Dynamic signature verification with template protection using helper data. In: Proceedings of the IEEE international conference on acoustics, speech, and signal processing, ICASSP, pp 1713–1716
17. Gomez-Barrero M, Galbally J, Morales A, Fierrez J (2017) Privacy-preserving comparison of variable-length data with application to biometric template protection. IEEE Access 5:8606–8619
18. Gomez-Barrero M, Maiorana E, Galbally J, Campisi P, Fierrez J (2017) Multi-biometric template protection based on homomorphic encryption. Pattern Recogn 67:149–163
19. Nanni L, Maiorana E, Lumini A, Campisi P (2010) Combining local, regional and global matchers for a template protected on-line signature verification system. Expert Syst Appl 37(5):3676–3684
20. Ponce-Hernandez W, Blanco-Gonzalo R, Liu-Jimenez J, Sanchez-Reillo R (2020) Fuzzy vault scheme based on fixed-length templates applied to dynamic signature verification. IEEE Access 8:11152–11164
21. Tolosana R, Vera-Rodriguez R, Ortega-Garcia J, Fierrez J (2015) Increasing the robustness of biometric templates for dynamic signature biometric systems. In: Proceedings of the 49th annual international carnahan conference on security technology
22. Malallah FL, Ahmad SS, Yussof S, Adnan W, Iranmanesh V, Arigbabu O (2013) A review of biometric template protection techniques for online handwritten signature application. Int Rev Comput Softw 8(12):1–9
23. Tolosana R, Vera-Rodriguez R, Gonzalez-Garcia C, Fierrez J, Morales A, Ortega-Garcia J, Carlos Ruiz-Garcia J, Romero-Tapiador S, Rengifo S, Caruana M, Jiang J, Lai S, Jin L, Zhu Y, Galbally J, Diaz M, Angel Ferrer M, Gomez-Barrero M, Hodashinsky I, Sarin K, Slezkin A, Bardamova M, Svetlakov M, Saleem M, Lia Szcs C, Kovari B, Pulsmeyer F, Wehbi M, Zanca D, Ahmad S, Mishra S, Jabin S (2022) Svc-ongoing: signature verification competition. Pattern Recogn 127:108,609
24. Nagel R, Rosenfeld A (1977) Computer detection of freehand forgeries. IEEE Trans Comput C-26:895–905
25. Gomez-Barrero M, Galbally J, Fierrez J, Ortega-Garcia J, Plamondon R (2015) Enhanced on-line signature verification based on skilled forgery detection using sigma-lognormal features. In: Proceedings of the IEEE/IAPR international conference on biometrics, ICB, pp 501–506
26. O'Reilly C, Plamondon R (2009) Development of a sigma-lognormal representation for on-line signatures. Pattern Recogn 42(12):3324–3337
27. Fierrez J, Morales A, Vera-Rodriguez R, Camacho D (2018) Multiple classifiers in biometrics. Part 1: fundamentals and review. Inf Fus 44:57–64
28. Sanchez-Reillo R, Quiros-Sandoval H, Goicochea-Telleria I, Ponce-Hernandez W (2017) Improving presentation attack detection in dynamic handwritten signature biometrics. IEEE Access 5:20463–20469
29. Madasu V, Lovell B (2008) An automatic off-line signature verification and forgery detection system In: Verma B, Blumenstein M (eds), Pattern recognition technologies and applications: recent advances, IGI Global, pp 63–88
30. Brault J, Plamondon R (1993) A complexity measure of handwritten curves: modeling of dynamic signature forgery. IEEE Trans Syst Man Cybern 23:400–413
31. Wu X, Kimura A, Iwana BK, Uchida S, Kashino K (2019) Deep dynamic time warping: end-to-end local representation learning for online signature verification. In: 2019 international conference on document analysis and recognition (ICDAR). IEEE, pp 1103–1110

32. Vorugunti CS, Mukherjee P, Pulabaigari V et al (2019) OSVNet: convolutional siamese network for writer independent online signature verification. In: 2019 international conference on document analysis and recognition (ICDAR). IEEE, pp 1470–1475
33. Lai S, Jin L, Zhu Y, Li Z, Lin L (2021) SynSig2Vec: forgery-free learning of dynamic signature representations by sigma lognormal-based synthesis. IEEE Trans Pattern Anal Mach Intell
34. Tolosana R, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J (2018) Exploring recurrent neural networks for on-line handwritten signature biometrics. IEEE Access 1–11
35. Caruana M, Vera-Rodriguez R, Tolosana R (2021) Analysing and exploiting complexity information in on-line signature verification. In: Proceedings of the international conference on pattern recognition workshops, ICPRw
36. Vera-Rodriguez R, Tolosana R, Caruana M, Manzano G, Gonzalez-Garcia C, Fierrez J, Ortega-Garcia J (2019) DeepSignCX: signature complexity detection using recurrent neural networks. In: Proceedings of the 15th international conference on document analysis and recognition, ICDAR
37. Doddington G, Liggett W, Martin A, Przybocki M, Reynolds D (1998) Sheeps, goats, lambs and wolves: a statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation. In: Proceedings of the international conference on spoken language processing
38. Yager N, Dunstone T (2010) The biometric menagerie. IEEE Trans Pattern Anal Mach Intell 32(2):220–230
39. Houmani N, Garcia-Salicetti S (2016) On hunting animals of the biometric menagerie for online signature. PLoS ONE 11(4):1–26
40. Ortega-Garcia J, Fierrez-Aguilar J, Simon D, Gonzalez J, Faundez-Zanuy M, Espinosa V, Satue A, Hernaez I, Igarza JJ, Vivaracho C et al (2003) MCYT baseline corpus: a bimodal biometric database. IEE Proc-Vis Image Signal Process 150(6):395–401
41. Ballard L, Lopresti D, Monroe F (2007) Forgery quality and its implication for behavioural biometric security. IEEE Trans Syst Man Cybernet Part B 37(5):1107–1118
42. Vielhauer C, Zöbisch F (2003) A test tool to support brute-force online and offline signature forgery tests on mobile devices. In: Proceedings of the international conference multimedia and expo, vol 3, pp 225–228
43. Alonso-Fernandez F, Fierrez J, Gilperez A, Galbally J, Ortega-Garcia J (2009) Robustness of signature verification systems to imitators with increasing skills. In: Proceedings of the 10th international conference on document analysis and recognition
44. Ferrer M, Diaz M, Carmona-Duarte C, Morales A (2017) A behavioral handwriting model for static and dynamic signature synthesis. IEEE Trans Pattern Anal Mach Intell 39(6):1041–1053
45. Fierrez J, Galbally J, Ortega-Garcia J et al (2010) BiosecurID: a multimodal biometric database. Pattern Anal Appl 13(2):235–246
46. Fierrez-Aguilar J, Alonso-Hermira N, Moreno-Marquez G, Ortega-Garcia J (2004) An off-line signature verification system based on fusion of local and global information. In: Proceedings of the European conference on computer vision, workshop on biometric authentication, BIOAW, LNCS, vol 3087. Springer, pp 295–306
47. Tolosana R, Vera-Rodriguez R, Ortega-Garcia J, Fierrez J (2015) Update strategies for HMM-based dynamic signature biometric systems. In: Proceedings of the 7th IEEE international workshop on information forensics and security, WIFS
48. Graves A (2013) Generating sequences with recurrent neural networks. arXiv:1308.0850
49. Ferrer MA, Diaz M, Carmona-Duarte C, Plamondon R (2018) iDeLog: Iterative dual spatial and kinematic extraction of sigma-lognormal parameters. IEEE Trans Pattern Anal Mach Intell 42(1):114–125
50. Vera-Rodriguez R, Tolosana R, Hernandez-Ortega J, Acien A, Morales A, Fierrez J, Ortega-Garcia J (2020) Modeling the complexity of signature and touch-screen biometrics using the lognormality principle. World Scientific, pp 65–86
51. Diaz M, Fischer A, Ferrer M, Plamondon R (2016) Dynamic signature verification system based on one real signature. IEEE Trans Cybernet 48:228–239
52. Galbally J, Fierrez J, Martinez-Diaz M, Ortega-Garcia J (2009) Improving the enrollment in dynamic signature verification with synthetic samples. In: Proceedings of the IAPR international conference on document analysis and recognition, ICDAR, pp 1295–1299

53. Lai S, Jin L, Lin L, Zhu Y, Mao H (2020) SynSig2Vec: learning representations from synthetic dynamic signatures for real-world verification. In: Proceedings of the AAAI conference on artificial intelligence, vol 34, pp 735–742
54. Tolosana R, Delgado-Santos P, Perez-Uribe A, Vera-Rodriguez R, Fierrez J, Morales A (2021) DeepWriteSYN: on-line handwriting synthesis via deep short-term representations. In: Proceedings AAAI conference on artificial intelligence
55. Carmona-Duarte C, Ferrer MA, Parziale A, Marcelli A (2017) Temporal evolution in synthetic handwriting. Pattern Recogn 68:233–244
56. Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J (2019) Do you need more data? The DeepSignDB on-line handwritten signature biometric database. In: Proceedings international conference on document analysis and recognition (ICDAR)
57. Houmani N, Mayoue A, Garcia-Salicetti S, Dorizzi B, Khalil M, Moustafa M, Abbas H, Muramatsu D, Yanikoglu B, Kholmatov A, Martinez-Diaz M, Fierrez J, Ortega-Garcia J, Alcobé JR, Fabregas J, Faundez-Zanuy M, Pascual-Gaspar J, Cardeñoso-Payo V, Vivaracho-Pascual C (2012) Biosecure signature evaluation campaign (BSEC'2009): evaluating on-line signature algorithms depending on the quality of signatures. Pattern Recogn 45(3):993–1003
58. Martinez-Diaz M, Fierrez J, Krish R, Galbally J (2014) Mobile signature verification: feature robustness and performance comparison. IET Biom 3(4):267–277
59. Martinez-Diaz M, Fierrez J, Hangai S (2015) Signature matching. In: Li SZ, Jain A (eds), Encyclopedia of biometrics. Springer, pp 1382–1387
60. Tekampe N, Merle A, Bringer J, Gomez-Barrero M, Fierrez J, Galbally J (2016) Toward common criteria evaluations of biometric systems. Technical Report BEAT Public Deliverable D6.5. https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems