Chapter 19
Presentation Attacks in Signature Biometrics: Types and Introduction to Attack Detection

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

Abstract Authentication applications based on the use of biometric methods have received a lot of interest during 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 work carries out an analysis of different Presentation Attack (PA) scenarios for on-line handwritten signature verification. The main contributions of the present work are: (1) short overview of representative methods for Presentation Attack Detection (PAD) in signature biometrics; (2) to describe the different levels of PAs existing in on-line signature verification regarding the amount of information available to the attacker, as well as the training, effort and ability to perform the forgeries; and (3) to report an evaluation of the system performance in signature biometrics under different PAs and writing tools considering freely available signature databases. Results obtained for both BiosecurID and e-BioSign 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. 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.

R. Tolosana (✉) · R. Vera-Rodriguez · 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
Universidad Autonoma de Madrid, 28049 Madrid, Spain
e-mail: julian.fierrez@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/10.1007/978-3-319-92627-8_19

19.1 Introduction

Applications based on biometric user authentication have experienced a high deployment in many relevant sectors such as security, e-government, healthcare, education, banking or insurance in the last years [1]. This growth has been possible thanks to two main factors: (1) the technological evolution and the improvement of sensors quality [2], which have cut the prices of general purpose devices (smartphones and tablets) and therefore, the high acceptance of the society towards the use of them; and (2) the evolution of biometric recognition technologies in general [3–5]. However, it is important to keep in mind that these biometric-based authentication systems have to withstand different types of possible attacks [6].

In this work, we focus on different Presentation Attack (PA) scenarios for online handwritten signature biometric authentication systems. These systems have received a significant amount of attention in the last years thanks to improved signature acquisition scenarios (including device interoperability [7]) and writing inputs (e.g. finger [8]).

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 user being attacked is known and impostors present their own signature claiming to be another user of the system, and (2) *skilled* impostors, the case in which impostors have some level of information about the user being attacked (e.g. image of the signature) and try to forge their signature claiming to be that user in the system.

Galbally et al. have recently discussed in [9] different approaches to report accuracy results in handwritten signature verification applying the lessons learned in the evaluation of vulnerabilities to Presentation Attacks (PAs). They considered skilled impostors as a particular case of biometric PAs that is performed against a behavioral biometric characteristic (referred to in some cases as *mimicry*). It is important to highlight the key differences between physical PAs and mimicry, while traditional PAs involve the use of some physical artefacts such as fake masks and gummy fingers (and therefore, 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 normal access attempt. Galbally et al. in [9] modified the traditional nomenclature of impostor scenarios in signature verification (i.e. skilled and random) following the standard in the field of biometric Presentation Attack Detection (PAD). This way, the classical random impostor scenario was referred to as Bona Fide (BF) scenario, while the skilled impostor scenario was referred to as PA scenario. This new nomenclature is used in this chapter as well.

If those PAs are expected, one can include specific modules for PAD, which in the signature recognition literature are usually referred to as forgery detection modules. A survey of such PAD methods is out of the scope of the chapter. Here in Sect. 19.2, we only provide a short overview of some selected representative works in that area.

A different approach aimed at improving the security against attacks in signature biometrics different from including a PAD module is template protection [10].

Traditional on-line signature verification systems use very sensitive biometric data such as the X and Y spatial coordinates for the matching, storing this information as the user templates without any kind of protection. A compromised template, in this case, would easily provide an attacker with the X and Y coordinates along the time axis, making possible to generate very high-quality forgeries of the original signature. In [11], an 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 that store very sensitive information.

The main contributions of the present work are: (1) short overview of representative methods for PAD in signature biometrics; (2) to describe the different levels of PAs existing in on-line signature verification regarding the amount of information available to the attacker, as well as the training, effort and ability to perform the forgeries; and (3) to report an evaluation of the system performance in signature biometrics under different PAs and writing tools considering freely available signature databases.

The remainder of the chapter is organized as follows. The introduction is completed with a short overview of PAD in signature biometrics (Sect. 19.2). After that, the main technical content of the chapter begins in Sect. 19.3, with a review of the most relevant possible attacks, pointing out which type of impostors are included in various well-known public signature databases. Section 19.4 describes the on-line signature databases considered in the experimental work. Section 19.5 describes the experimental protocol and the results achieved. Finally, Sect. 19.6 draws the final conclusions and points out some lines for future work.

19.2 PAD in Signature Biometrics

Presentation Attack Detection (PAD) in signature biometrics can be traced back to early works by Rosenfeld et al. in the late 70s [12]. In that work, authors dealt with the detection of freehand forgeries (i.e. forgeries written in the forger's own handwriting without knowledge of the appearance of the genuine signature) on bank checks for off-line signature verification. The detection process made use of features derived from Eden's model [13], which characterizes handwriting strokes in terms of a set of kinematic parameters that can be used to discriminate forged from genuine signatures. Those features were based on dimension ratios and slant angles, measured for the signature as a whole and for specific letters on it. Finally, unknown signatures were classified as genuine or forgery on the basis of their distance from the set of genuine signatures. A more exhaustive analysis was later carried out in [14], performing skilled forgery detection by examining the writer-dependent information embedded at the substroke level and trying to capture unballistic motion and tremor information in each stroke segment, rather than as global statistics.

In [15], 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 et al. presented in [16] 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 application as well. This work supposed 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 inch.

More studies of PAD methods at feature level for on-line signature verification were carried out in [17, 18]. In [17], authors proposed a new scheme in which a module focused on the detection of skilled forgeries (i.e. PA impostors) was added to the original verification system. That new module (i.e. Skilled Forgeries Detector) was based on four parameters of the Sigma LogNormal writing generation model [19] and a linear classifier. That new binary classification module was supposed to work sequentially before a standard signature recognition system [20]. Good results were achieved using that approach for both skilled (i.e. PA) and random (i.e. BF) scenarios. In [18], 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 reduced the EER from a percentage close to 20.0% to below 3.0%.

19.3 Presentation Attacks in Signature Biometrics

This section aims to describe the different levels of skilled forgeries (i.e. PA impostors) that exist in the literature regarding the amount of information provided to the attacker, as well as the training, effort and ability to perform the forgeries. In addition, we consider the case of random forgeries (i.e. zero-effort impostors) although it belongs to the BF scenario and not to the PA scenario in order to review the whole range of possible impostors in handwritten 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 [21], classifying speakers regarding how easy or difficult the speaker can be recognized (i.e. sheep and goats, respectively), how easily they can be forged (i.e. lambs) and finally, how good they are forging others (i.e. wolves). Yager and Dunstone have more recently extended the Biometric Menagerie in [22] 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 [23], 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 [24], where the attacker had access to a visual static image of the signature to forge.

In [25], authors showed through a series of experiments that: (1) some users are significantly better forgers than others (these users would be classified as wolves in the previous user categorization); (2) forgers can be trained in a relatively straightforward way to become a greater threat; (3) certain users are easy targets for forgers (sheep following the previous user categorization); 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: *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 defined trained and generative impostors as skilled forgeries (i.e. PA impostors) when only the image or the dynamics of the signature to forge is available, respectively.

In [26], authors proposed a software tool implemented on two different computer platforms in order to generate 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. 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 average quadratic deviation. Results obtained for four different threshold values confirmed a strong protection against attacks.

A more exhaustive analysis of the different types of forgeries possible in signature recognition was carried out in [27]. In that work, authors considered random or zero-effort impostors plus four different levels of PA impostors regarding the amount of information provided to the attacker and the tools used for the impostors in order to forge the signature:

- **Random or zero-effort forgeries**, in which no information of the user to forge is available and the impostor uses its own signature (accidentally or not) claiming to be another user of the system.
- **Blind forgeries**, in which the attacker has access to a descriptive or textual knowledge of the original signatures (e.g. the name of the person).
- **Static forgeries** (low-force in [26]), where the attacker has access to a visual static image of the signature to forge. There are two ways to generate the forgeries. 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, leading to **static trained forgeries**. In the second one, the attacker uses a blueprint to first copy the 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 the same appearance as the original ones.
- **Dynamic forgeries** (brute-force in [26]), where the attacker has access to both the 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 dedicated 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 needs to follow.
- **Regained forgeries**, the case where the attacker has access only to the static image of the signature to forge and makes use of a dedicated software to regain its dynamics [28], which are later analyzed and used to create dynamic forgeries.

Figure 19.1 depicts examples of one 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 [27], Alonso-Fernandez et al. studied the impact of an incremental level of quality in the PAs against signature verification systems. Both off-line and on-line systems were considered using the BiosecurID database which contains both off-line and on-line signatures. For the off-line system, they considered a system based on global image analysis and a minimum distance classifier [29] whereas a system based on Hidden Markov Models (HMM) [30] was considered for the on-line approach. Their experiments concluded that the

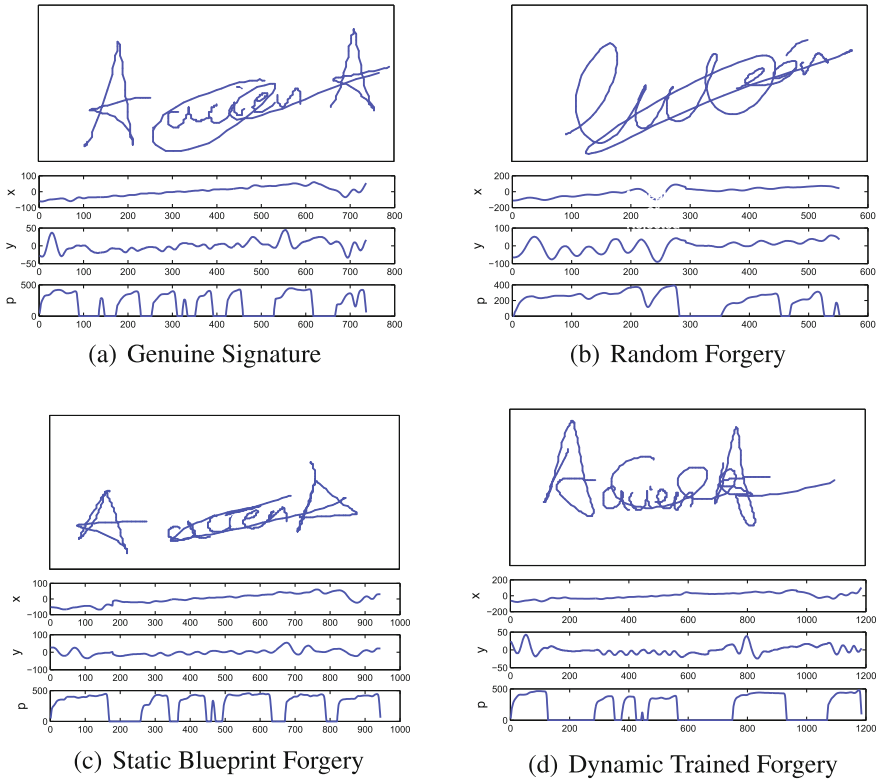


Fig. 19.1 Examples of one genuine signature and three different types of forgeries performed for the same user

performance of the off-line system is only degraded with the highest level of forgeries quality. On the contrary, the on-line system exhibits a progressive degradation with the forgeries quality, suggesting that the dynamic information of signatures is the one more affected by the considered increased forgeries quality.

Finally, Fig. 19.2 summarizes all different types of forgeries for both BF and PA scenarios regarding the amount of information available to the attacker, as well as the training, effort and ability to perform the attack. In addition, the most commonly used on-line signature databases are included in each PA group. It is important to highlight the lack of public on-line signature databases for the case of blind forgeries, as far as we know.

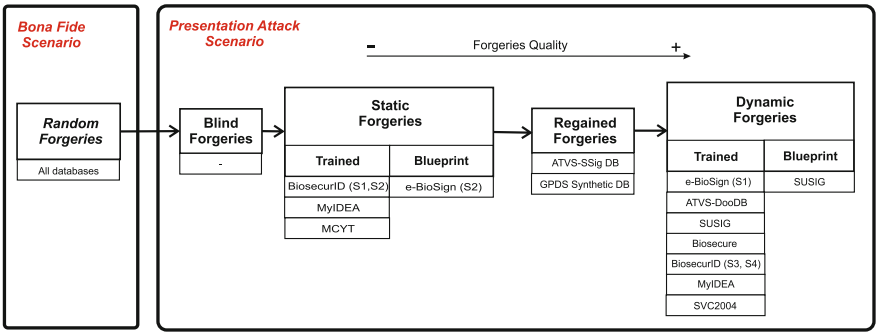


Fig. 19.2 Diagram of different types of forgeries for both BF and PA scenarios regarding the amount of information available to the attacker, as well as the training, effort and ability to perform the attack. The commonly used on-line signature databases are included in each PA group

19.4 On-Line Signature Databases

The following two databases are considered in the experiments reported here:

19.4.1 e-BioSign

For the e-BioSign database [8], we consider a subset of the freely available database[1] comprised of signatures acquired using a Samsung ATIV 7 general purpose device (a.k.a. W4 device). The W4 device has a 11.6-inch LED display with a resolution of 1920×1080 pixels and 1024 pressure levels. Data was collected using a pen stylus and also the finger in order to study the performance of signature verification in a mobile scenario. The available information when using the pen stylus is X and Y pen coordinates and pressure. In addition, pen-up trajectories are also available. However, for the case of using the finger as the writing tool, pressure information and pen-ups trajectories are not recorded. Regarding the acquisition protocol, the device was placed on a desktop and subjects were able to rotate the device in order to feel comfortable with the writing position.

Data were collected in two sessions for 65 subjects with a time gap between sessions of at least three weeks. For each user and writing tool, there are a total of eight genuine signatures and six skilled forgeries (i.e. PA impostors). Regarding skilled forgeries for the case of using the stylus as the writing tool, users were allowed during the first session to visualize a recording of the dynamic realization of the signature to forge as many times as they wanted whereas only the image of the signature to forge was available during the second session. Regarding skilled forgeries for the case of using the finger as the writing tool, in both sessions users

[1] https://atvs.ii.uam.es/atvs/eBioSign-DS1.html.

had access to the dynamic realization of the signatures to forge as many times as they wanted.

19.4.2 BiosecurID

For the BiosecurID database [31], we consider a subset [32] comprised of a total of 132 users.[2] Signatures were acquired using a Wacom Intuos 3 pen tablet with a resolution of 5080 dpi and 1024 pressure levels. The database comprises 16 genuine signatures and 12 skilled forgeries (i.e. PA impostors) per user, captured in four separate acquisition sessions. Each session was captured leaving a two-month interval between them, in a controlled and supervised office-like scenario. Signatures were acquired using a pen stylus. The available information within each signature is X and Y pen coordinates and pressure. In addition, pen-up trajectories are available.

The following PAs are considered in the database in order to analyze how the system performance differs regarding the amount of information provided to the attacker: (i) the attacker only sees the image of the signature once and tries to imitate it right away (session 1); (ii) the attacker sees the image of the signature and trains for a minute before making the forgery (session 2); (iii) the attacker is able to see the dynamics of the signing process three times, trains for a minute and then makes the forgery (session 3); and (iv) the dynamics of the signature are shown as many times as the attacker requests, being able to train for a minute and then sign (session 4).

19.5 Experimental Work

19.5.1 Signature Verification System

An on-line signature verification system based on time functions (a.k.a. local systems) is considered in the experimental work [33]. For each signature acquired using the stylus or the finger, only signals related to X and Y pen coordinates and their first- and second-order derivatives are used in order to provide reproducible results. Information related to pen angular orientation (azimuth and altitude angles) and pressure have been always discarded in order to consider the same set of time functions that we would be able to use in general purpose devices such as tablets and smartphones using the finger as the writing tool.

Our local system is based on DTW, which computes the similarity between the time functions from the input and training signatures. The configuration of the DTW algorithm described in [34].

[2] https://atvs.ii.uam.es/atvs/biosecurid_sonof_db.html.

19.5.2 Experimental Protocol

The experimental protocol has been designed to allow the study of both BF and PA scenarios on the system performance. Three different levels of impostors are analyzed: (1) random forgeries, (2) static forgeries (both trained and blueprint) and (3) dynamic forgeries. Additionally, for the e-BioSign subset, the case of using the finger as the writing tool is considered. All available users (i.e. 65 and 132 for e-BioSign and BiosecurID subsets, respectively) are used for the evaluation as no development of the on-line signature verification system is carried out.

For both databases, the four genuine signatures of the first session are used as reference signatures, whereas the remaining genuine signatures (i.e. 4 and 12 for the e-BioSign and BiosecurID databases, respectively) are used for testing. Skilled forgeries scores (i.e. PA mated scores) are obtained by comparing the reference signatures against the skilled forgeries (i.e. PA impostors) related to each level of attacker, whereas random forgeries scores (i.e. BF non-mated scores) are obtained by comparing the reference signatures with one genuine signature of each of the remaining users (i.e. 64 and 131 for the e-BioSign and BiosecurID databases, respectively). The final score is obtained after performing the average score of the four one-to-one comparisons.

19.5.3 Experimental Results

Tables 19.1 and 19.2 show the system performance obtained for each different type of impostor and database. Additionally, Fig. 19.3 shows the system performance in terms of DET curves for each impostor scenario and database.

First, we analyze the results achieved for the case of using the stylus as the writing tool. In this case, a system performance improvement can be observed for both BiosecurID (Table 19.1) and e-BioSign (Table 19.2) databases when the amount of information that the attacker has is reduced. For example, a 7.5% EER is obtained in Table 19.1 when the attacker has access to the dynamics and also the static information

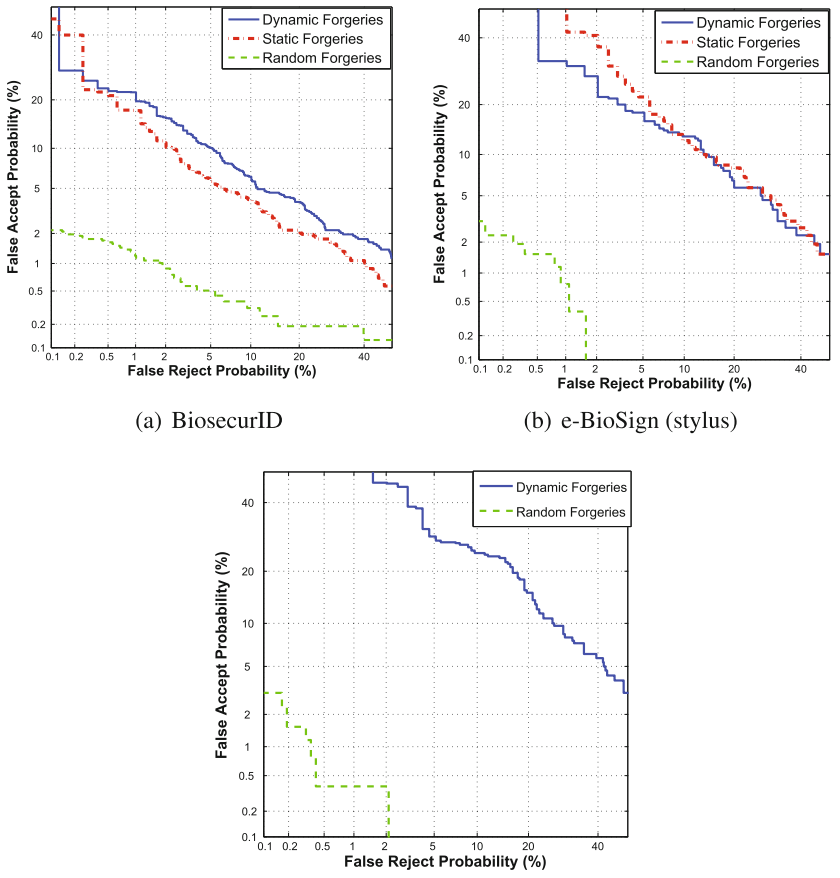
Table 19.1 BiosecurID: system performance results (EER in %)

	Random forgeries	Static forgeries	Dynamic forgeries
Stylus	1.1	5.4	7.5

Table 19.2 e-BioSign: system performance results (EER in %)

	Random forgeries	Static forgeries	Dynamic forgeries
Stylus	1.0	11.4	12.3
Finger	0.4	8.9*	18.3

*Generated on new data captured after e-BioSign



(a) BiosecurID

(b) e-BioSign (stylus)

(c) e-BioSign (finger)

Fig. 19.3 System performance results obtained for each different type of impostor and database

of the signature to forge whereas this value is reduced to 5.4% EER when only the static information is provided to the forger.

We can also observe the impact of varying training and effort to perform the forgeries by comparing Tables 19.1 and 19.2. In general, higher errors are observed for the e-BioSign database for both types of skilled forgeries (i.e. dynamic and static) compared to the BiosecurID database. This is due to the fact that for dynamic forgeries, the attackers of the e-BioSign database had access to the dynamic realization of the signatures to forge as many times as they wanted and were also allowed to train without restrictions of time, whereas for the BiosecurID database the attackers had time restrictions, resulting in lower quality forgeries. For the case of static forgeries, the attackers of the e-BioSign database used a blueprint with the image of the signature to forge, placing it on the screen of the device while forging whereas for

the BiosecurID database, the attackers just saw the image of the signatures to forge and trained before making the forgery without the help of any blueprint.

Finally, very similar good results are achieved in Tables 19.1 and 19.2 for random forgeries (i.e. zero-effort impostors) as the attackers have no information of the user to forge and present to the system their own signature.

Analyzing the case of using the finger as the writing tool, a high degradation of the system performance can be observed in Table 19.2 for the dynamic forgeries compared to the case of using the stylus as the writing tool. A recommendation for the usage of signature recognition on mobile devices would be for the users to protect themselves from other people that could be watching while signing, as this is more feasible to do in a mobile scenario compared to an office scenario. This way skilled forgers (i.e. PA impostors) might have access to the global shape of the signature but not to the dynamic information and results would be much better. For analyzing this scenario, we captured additional data after e-BioSign achieving a 8.9% EER (marked with * in Table 19.2, as the dataset in this case is not the same of the rest of the table), much better results compared to the 18.3% EER obtained for dynamic forgeries. For the case of random forgeries (i.e. zero-effort impostors), better results are obtained when the finger is considered as the writing tool compared to the stylus proving the feasibility of this scenario for random forgeries. Finally, it is important to remind that we are using a simple and reproducible verification system based only on X, Y coordinates and their derivatives. For a complete analysis of using the finger as the writing tool please refer to [8].

Finally, we would like to remark that the results obtained in this work should be interpreted in general terms as comparing different scenarios of attack. Specific results on operational setups can vary depending on the specific matching algorithm considered. An example of this can be seen in [35], where two different verification systems (i.e. Recurrent Neural Networks (RNNs) and DTW) were evaluated on the BiosecurID database for different types of attacks. The signature verification system based on RNNs obtained much better results than DTW for skilled forgeries, but DTW outperformed RNNs for random forgeries concluding that fusion of both systems could be a good strategy. Similar conclusions can be observed in previous studies [36, 37].

19.6 Conclusions

This work carries out an analysis of Presentation Attack (PA) scenarios [6] for on-line handwritten signature verification [33]. Unlike traditional PAs, which use physical artefacts (e.g. fake masks and gummy fingers), the most typical PAs in signature verification represent an attacker interacting with the sensor exactly in the same way followed in a normal access attempt, i.e. the presentation attack is a handwritten signature, in this case imitating to some extent the attacked identity. In such typical PA scenario, the level of knowledge that the attacker has and uses about the signature being attacked results crucial for the success rate of the attack.

The main contributions of the present work are: (1) short overview of representative methods for PAD in signature biometrics; (2) to describe the different levels of PAs existing in on-line signature verification regarding the amount of information available to the attacker, as well as the training, effort and ability to perform the forgeries and (3) to report an evaluation of the system performance in signature biometrics under different PAs and writing tools considering available signature databases.

Results obtained for both BiosecurID [31] and e-BioSign [8] 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 [27]. For the case of using the finger as the writing tool, a recommendation for the usage of signature recognition on mobile devices would be for the users to protect themselves from other people that could be watching while signing, as this is more feasible to do in a mobile scenario [38] compared to an office scenario. This way skilled forgers (i.e. PA impostors) might have access to the global shape of the signature but not to the dynamic information and results 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 [39].

Acknowledgements This work has been supported by projects: Bio-Guard (Ayudas Fundación BBVA a Equipos de Investigación Científica 2017), UAM-CecaBank, and by TEC2015-70627-R (MINECO/FEDER). Ruben Tolosana is supported by a FPU Fellowship from the Spanish MECD.

References

1. Meng W, Wong DS, Furnell S, Zhou J (2015) Surveying the development of biometric user authentication on mobile phones. IEEE Commun Surv Tutor 17:1268–1293
2. Zhang DD (2013) Automated biometrics: technologies and systems. Springer Science & Business Media, Berlin
3. Jain AK, Nandakumar K, Ross A (2016) 50 Years of biometric research: accomplishments, challenges, and opportunities. Pattern Recognit Lett 79:80–105
4. Taigman Y, Yang M, Ranzato MA, Wolf L (2014) Deepface: closing the gap to human-level performance in face verification. In: The IEEE conference on computer vision and pattern recognition (CVPR)
5. Impedovo D, Pirlo G (2008) Automatic signature verification: the state of the art. IEEE Trans Syst Man Cybern Part C (Appl Rev) 38(5):609–635
6. 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
7. 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
8. 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 12(5):e0176792

9. Galbally J, Gomez-Barrero M, Ross A (2017) Accuracy evaluation of handwritten signature verification: rethinking the random-skilled forgeries dichotomy. In Proceedings of IEEE international joint conference on biometrics, pp 302–310
10. 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
11. 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 49th annual international Carnahan conference on security technology
12. Nagel RN, Rosenfeld A (1977) Computer detection of freehand forgeries. IEEE Trans Comput C-26:895–905
13. Eden M (1961) On the formalization of handwriting. Structure of language and its mathematical aspects (Proceedings of symposia in applied mathematics), vol 12. American Mathematical Society, Providence, pp 83–88
14. Guo JK, Doermann D, Rosenfeld A (2001) Forgery detection by local correspondence. Int J Pattern Recognit Artif Intell 15
15. Madasu VK, Lovell BC (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, USA, pp 63–88
16. Brault JJ, Plamondon R (1993) A complexity measure of handwritten curves: modeling of dynamic signature forgery. IEEE Trans Syst Man Cybern 23:400–413
17. Gomez-Barrero M, Galbally J, Fierrez J, Ortega-Garcia J, Plamondon R (2015) Enhanced online signature verification based on skilled forgery detection using sigma-lognormal features. In: Proceedings of IEEE/IAPR international conference on biometrics. ICB, pp 501–506
18. Sanchez-Reillo R, Quiros-Sandoval HC, Goicochea-Telleria I, Ponce-Hernandez W (2017) Improving presentation attack detection in dynamic handwritten signature biometrics. IEEE Access 5:20463–20469
19. O'Reilly C, Plamondon R (2009) Development of a sigma-lognormal representation for on-line signatures. Pattern Recognit 42(12):3324–3337
20. Fierrez J, Morales A, Vera-Rodriguez R, Camacho D (2018) Multiple classifiers in biometrics. part 1: fundamentals and review. Inf Fusion 44:57–64
21. 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 international conference on spoken language processing
22. Yager N, Dunstone T (2010) The biometric menagerie. IEEE Trans Pattern Anal Mach Intell 32(2):220–230
23. Houmani N, Garcia-Salicetti S (2016) On hunting animals of the biometric menagerie for online signature. PLoS ONE 11(4):e0151691
24. Ortega-Garcia J, et al. (2003) MCYT baseline corpus: a bimodal biometric database. IEE Proc Vis Image Signal Process Spec Issue Biom Internet 150(6):395–401
25. Ballard L, Lopresti D, Monroe F (2007) Forgery quality and its implication for behavioural biometric security. IEEE Trans Syst Man Cybern Part B 37(5):1107–1118
26. Vielhauer C, Zbisch F (2003) A test tool to support brute-force online and offline signature forgery tests on mobile devices. In: Proceedings of international conference on multimedia and expo, vol 3, pp 225–228
27. 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 10th international conference on document analysis and recognition, pp 728–732
28. Ferrer MA, 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
29. 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 European conference on computer vision, workshop on biometric authentication, BIOAW, LNCS, vol. 3087. Springer, Berlin, pp 295–306

30. Tolosana R, Vera-Rodriguez R, Ortega-Garcia J, Fierrez J (2015) Update strategies for HMM-based dynamic signature biometric systems. In: Proceedings of 7th IEEE international workshop on information forensics and security, WIFS
31. Fierrez J, Galbally J, Ortega-Garcia J, et al. (2010) BiosecurID: a multimodal biometric database. Pattern Anal Appl 13(2):235–246
32. Galbally J, Diaz-Cabrera M, Ferrer MA, Gomez-Barrero M, Morales A, Fierrez J (2015) On-line signature recognition through the combination of real dynamic data and synthetically generated static data. Pattern Recognit 48:2921–2934
33. Martinez-Diaz M, Fierrez J, Hangai S (2015) Signature features. In: Li SZ, Jain A (eds) Encyclopedia of biometrics. Springer, Berlin, pp 1375–1382
34. Martinez-Diaz M, Fierrez J, Hangai S (2015) Signature matching. In: Li SZ, Jain A (eds) Encyclopedia of biometrics. Springer, Berlin, pp 1382–1387
35. Tolosana R, Vera-Rodriguez R, Fierrez J, Ortega-Garcia J (2018) Exploring recurrent neural networks for on-line handwritten signature biometrics. IEEE Access 6:5128–5138
36. Liu Y, Yang Z, Yang L (2014) Online signature verification based on DCT and sparse representation. IEEE Trans Cybern 45:2498–2511
37. Diaz M, Fischer A, Ferrer MA, Plamondon R (2016) Dynamic signature verification system based on one real signature. IEEE Trans Cybern 48:228–239
38. Martinez-Diaz M, Fierrez J, Krish RP, Galbally J (2014) Mobile signature verification: feature robustness and performance comparison. IET Biom 3(4):267–277
39. Tekampe N, Merle A, Bringer J, Gomez-Barrero M, Fierrez J, Galbally J (2016) Toward Common Criteria evaluations of biometric systems. BEAT public deliverable D6.5. https://www.beat-eu.org/project/deliverables-public/d6-5-toward-common-criteria-evaluations-of-biometric-systems