Available online at www.rpnsci.com

ISSN (P): 3006-8452, ISSN (O): 3006-8460

Research Prospects in Natural Sciences, Vol. 3, Issue 1, (2025) 25–28

Research Article

Analysis of presentation attacks detection in signature biometrics

Kamila Rehman[a], Aaliya Rehman[a,b,*], Burhan Zamir[a]

[a]*Department of Physics, Govt. M.A.O. Graduate College, Lahore 54000, Pakistan*
[b]*University Malaysia Sabah, 88400 Kota Kinabalu, Sabah, Malaysia*

Abstract

Authentication of biometric methods using various applications such as face or fingerprint recognition have received a lot of interest recently. However, at the same time these biometric systems have been facing different types of attacks. The current work carries out an analysis of different Presentation Attack (PA) scenarios for on-line handwritten signature verification. The present work introduces a short summery of methods for Presentation Attack Detection (PAD) in signature biometrics in order 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. This work is an effort towards security evaluation of biometric systems, where attacks are rated depending on expertise of the attacker, as well as the information available and used from the target being attacked.

Keywords:
Presentation Attack Detection (PAD), On-line signature verification, Forgery.

1. Introduction

Applications relying on biometric user authentication have witnessed significant adoption across diverse sectors, including finance, healthcare, education, e-government, insurance, and security [1]. The surge in their popularity can be attributed to two major factors. Firstly, the advancement of sensor technology [2], leading to reduced costs of general-purpose devices like smartphones and tablets, which has increased societal acceptance. Secondly, the evolution of biometric recognition technologies in general [3–5]. However, it's crucial to acknowledge that these biometric-based authentication systems must be resilient against various potential attacks [6]. Our study primarily centers on exploring Presentation Attack (PA) scenarios concerning online handwritten signature biometric authentication systems. These systems have garnered considerable attention due to enhanced signature acquisition setups (including device interoperability [7]) and diverse writing inputs (e.g., finger [8]). In the context of signature verification, two types of impostors can be identified: (1) random (zero-effort or accidental) impostors, where the attacker possesses no information about the targeted user and presents their own signature as the user's, and (2) skilled impostors, who have some level of information about the targeted user (e.g., an image of the signature) and attempt to forge their signature to deceive the system.

Recently, Galbally et al. [9] discussed different approaches for reporting accuracy in handwritten signature verification, incorporating insights gained from evaluating vulnerabilities in Presentation Attacks (PAs). They considered skilled impostors as a particular case of biometric PAs, akin to mimicry, a behavioral biometric characteristic. Notably, the distinction between physical PAs and mimicry lies in the fact that traditional PAs involve the use of physical artifacts like fake masks and gummy fingers (which can sometimes be detected at the sensor level), whereas mimicry involves the exact interaction observed in a normal access attempt. To align with the biometric Presentation Attack Detection (PAD) field, Galbally et al. [9] modified the nomenclature for impostor scenarios in signature verification, referring to the classical random impostor scenario as Bona Fide (BF) scenario and the skilled impostor scenario as the PA scenario.

Another approach to enhance security against attacks in signature biometrics, apart from employing a PAD module, is template protection [10]. Conventional on-line signature verification systems use highly sensitive biometric data such as the X and Y spatial coordinates for matching, storing this information as user templates without any form of protection. A

*Corresponding Author:
aaliya.rehman@gmail.com (Aaliya Rehman)

compromised template in such a system could facilitate an attacker in generating high-quality forgeries of the original signature, as it provides the X and Y coordinates over time. A different approach [11] for signature template generation was proposed, omitting information related to X, Y coordinates and their derivatives, resulting in a more robust system against attacks, with comparable error rates to traditional systems that store sensitive information.

Subsequent studies [12] delved into PAD methods at the feature level for on-line signature verification. Yusof et. al. [13] introduced a new scheme that added a Skilled Forgeries Detector module to the original verification system. This module focused on detecting skilled forgeries based on four parameters of the Sigma LogNormal writing generation model and a linear classifier. The approach yielded promising results for both skilled (PA) and random (BF) scenarios. On the other hand, Reillo et al. [14] proposed PAD methods based on global features like the total number of strokes and signing time of signatures. They built a new database with 11 levels of PAs, and their proposed PAD significantly reduced the Equal Error Rate (EER).

Examining Different Levels of Presentation Attacks in Signature Biometrics: This section aims to explore various levels of skilled forgeries (PA impostors) found in the literature, considering the information available to the attacker, their training, effort, and forgery capabilities. Additionally, we consider random forgeries (zero-effort impostors), although they belong to the BF scenario, to encompass the entire range of possible impostors in handwritten signature verification.

Previous studies [15, 16]have applied the concept of Biometric Menagerie to categorize users of the biometric system based on animal classifications. The concept has been extended in recent research [17], considering various biometric modalities, including 2D and 3D faces, fingerprints, iris, speech, and keystroke dynamics. In on-line signature verification [16], the Biometric Menagerie concept was employed to classify users and quantify the difficulty of forging their signatures using personal and relative entropy measures.

Further research demonstrated [18] that some users are significantly better forgers (wolves) than others, and forgers can be trained to become a greater threat. Certain users are easy targets for forgers (sheep), and most individuals are relatively poor at judging handwriting authenticity. A new metric for impostor classification was proposed, distinguishing between naive, trained, and generative impostors.

Additional studies [19] developed software tools to generate forgeries of different quality levels (PA impostors). Three levels of PAs were considered: blind forgeries, low-force forgeries, and brute-force forgeries. The impact of an incremental level of quality in PAs against signature verification systems was examined, considering off-line and on-line systems using the BiosecurID database.

Overall, the field of Presentation Attack Detection in signature biometrics continues to evolve, with a focus on detecting skilled forgeries and enhancing security against various impostors to ensure reliable signature verification.

2. Materials and Methods

The experimental investigation focused on analyzing Presentation Attack (PA) scenarios in on-line handwritten signature verification [14]. A unique aspect of the research was the consideration of typical PAs in signature verification, where attackers interacted with the sensor in the same manner as a normal access attempt, involving a handwritten signature resembling the targeted identity as seen in Fig 1. The attacker's level of knowledge about the signature played a crucial role in the attack's success rate.

The experimental protocol allowed for the study of both BF and PA scenarios, involving three levels of impostors: (b) random forgeries, (c) static forgeries (trained and blueprint), and (d) dynamic forgeries. Additionally, the case of using the finger as the writing tool in the e-BioSign [20] subset was considered. All available users from the e-BioSign (65 users) and BiosecurID (132 users) subsets were used for evaluation, and no development of the on-line signature verification system was carried out.

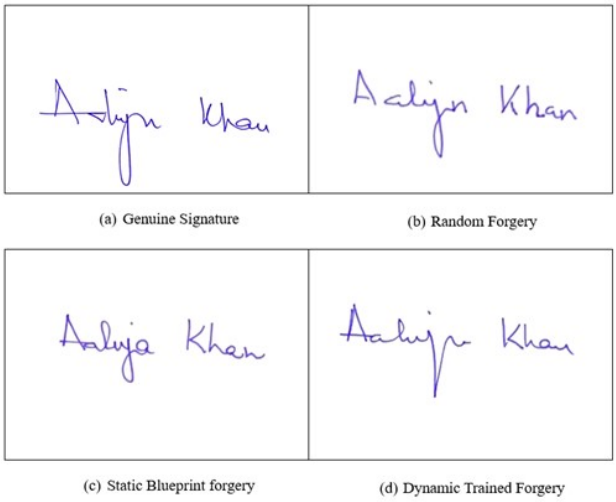

Figure 1: Four signature samples, including one genuine signature and three different types of forgeries, all produced for the same user

3. Results and Discussion

For both databases, genuine signatures from the first session served as reference signatures, and the remaining genuine signatures were used for testing. Skilled forgeries scores (PA mated scores) were obtained by comparing reference signatures against skilled forgeries for each level of attacker, while random forgeries scores (BF non-mated scores) were obtained by comparing reference signatures with genuine signatures from other users. The final score was determined by averaging the four one-to-one comparisons.

The experimental results for the stylus as the writing tool revealed improved system performance for both BiosecurID and e-BioSign databases when the attacker's available information

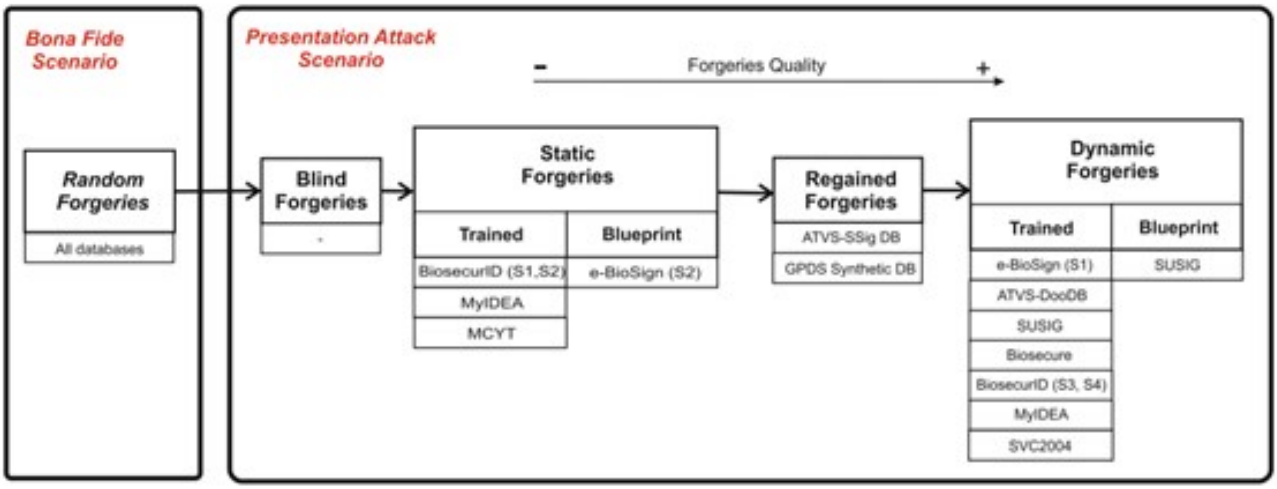

Figure 2: Illustration depicting the various forgery types for both BF and PA scenarios, considering the attacker´s available information, training, efforts, and ability to execute the attack.

was reduced. For example, an EER of 7.5% was achieved when the attacker had access to dynamics and static information, whereas it reduced to 5.4% when only static information was provided.

Varying training and effort to perform forgeries had an impact, with higher errors observed in the e-BioSign database for both dynamic and static skilled forgeries compared to the Biosecur ID database. The different scenarios and results for random forgeries (zero-effort impostors) showed similar good performance for both databases. When using the finger as writing tool, a significant degradation in system performance was observed for dynamic forgeries in the e-BioSign database compared to using the stylus. Protecting against potential onlookers while signing on mobile devices could improve results, as skilled forgers might not have access to dynamic information. Additional data captured after e-BioSign achieved a much better EER of 8.9% for dynamic forgeries compared to 18.3% in the original data set. Overall, the study emphasized that the results should be interpreted generally, as specific operational setups can influence outcomes depending on the matching algorithm used. Previous research has shown the efficacy of combining different verification systems to address various types of attacks.

4. Conclusion

In this study, an extensive examination of Presentation Attack (PA) scenarios in on-line handwritten signature verification was conducted. Unlike conventional PAs involving physical artifacts, the typical PAs observed in signature verification entail the attacker mimicking the normal access attempt closely, presenting a handwritten signature that imitates the targeted identity to some extent. The attacker's level of knowledge and its application to the signature being attacked significantly influenced the attack's success rate. The results obtained from both the Biosecur ID and e-BioSign databases revealed substantial effects on the system's performance, considering not only the attacker's information level but also their training and effort in executing the signature. When using the finger as writing tool, it is recommended for users to safeguard against potential onlookers while signing, especially in mobile scenarios. This precaution can significantly hinder skilled forgers (PA impostors) from accessing dynamic signature information, leading to much better outcomes.

References

[1] V. Podzorov, E. Menard, A. Borissov, V. Kiryukhin, J. A. Rogers, M. Gershenson, Intrinsic charge transport on the surface of organic semiconductors, Physical review letters 93 (8) (2004) 086602.

[2] F. Balzer, M. Schiek, A. Lützen, K. al-shamery, in: Proc. SPIE, Vol. 64706, 2007.

[3] Y. Luo, M. Brun, P. Rannou, B. Grevin, Growth of rubrene thin film, spherulites and nanowires on sio2, physica status solidi (a) 204 (6) (2007) 1851–1855.

[4] S. Seo, B.-N. Park, P. G. Evans, Ambipolar rubrene thin film transistors, Applied physics letters 88 (23).

[5] M. C. Scharber, D. Mühlbacher, M. Koppe, P. Denk, C. Waldauf, A. J. Heeger, C. J. Brabec, Design rules for donors in bulk heterojunction solar cells towards 10% energy conversion efficiency, Advanced materials 18 (6) (2006) 789–794.

[6] J. E. Norton, J. r me Cornil, V. Coropceanu, et al., Molecular understanding of organic solar cells: The challenges, Acc. Chem. Res. 42 (11) (2009) 1691–1699.

[7] C. W. Schlenker, M. E. Thompson, The molecular nature of photovoltage losses in organic solar cells, Chemical communications 47 (13) (2011) 3702–3716.

[8] S.-W. Park, J. M. Hwang, J.-M. Choi, D. Hwang, M. Oh, J. H. Kim, S. Im, Rubrene thin-film transistors with crystalline and amorphous channels, Applied physics letters 90 (15).

[9] J. Galbally, M. Gomez-Barrero, A. Ross, Accuracy evaluation of handwritten signature verification: Rethinking the random-skilled forgeries dichotomy, in: 2017 IEEE international joint conference on biometrics (IJCB), IEEE, 2017, pp. 302–310.

[10] C. Hsu, J. Deng, C. Staddon, P. Beton, Growth front nucleation of rubrene thin films for high mobility organic transistors, applied physics letters 91 (19).

[11] Y. C. Feng, P. C. Yuen, A. K. Jain, A hybrid approach for generating secure and discriminating face template, IEEE transactions on information forensics and security 5 (1) (2009) 103–117.
[12] J. Fierrez, J. Ortega-Garcia, On-line signature verification, in: Handbook of biometrics, Springer, 2008, pp. 189–209.
[13] M. H. M. Yusof, V. K. Madasu, Signature verification and forgery detection system, in: Proceedings. Student Conference on Research and Development, 2003. SCORED 2003., IEEE, 2003, pp. 9–14.
[14] R. Sanchez-Reillo, Signature analysis in the context of mobile devices, Image and Vision Computing 55 (2016) 34–37.
[15] N. Yager, T. Dunstone, The biometric menagerie, IEEE transactions on pattern analysis and machine intelligence 32 (2) (2008) 220–230.
[16] N. Houmani, S. Garcia-Salicetti, On hunting animals of the biometric menagerie for online signature, PloS one 11 (4) (2016) e0151691.
[17] S. Dargan, M. Kumar, A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities, Expert Systems with Applications 143 (2020) 113114.
[18] T. Diserens, J. Bubnicki, E. Schutgens, K. Rokx, R. Kowalczyk, D. Kuijper, M. Churski, Fossoriality in a risky landscape: Badger sett use varies with perceived wolf risk, Journal of Zoology 313 (1) (2021) 76–85.
[19] P. Sharma, M. Kumar, H. Sharma, Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation, Multimedia Tools and Applications 82 (12) (2023) 18117–18150.
[20] P. Craddock, Scientific investigation of copies, fakes and forgeries, Routledge, 2009.