Scientific Letters

Poster Communication 87

From fingerprints to spoofs: a systematic review of real-life spoofing cases

Maria L. V. Peixoto [1,2*], Soraia Nunes [1,2], Pedro Correia [3], Rui M. S. Azevedo [1,2], Áurea Madureira-Carvalho [1,2]

[1] Associate Laboratory i4HB – Institute for Health and Bioeconomy, University Institute of Health Sciences – CESPU, 4585-116 Gandra, Portugal
[2] UCIBIO – Research Unit on Applied Molecular Biosciences, Forensic Science Research Laboratory, University Institute of Health Sciences (1H-TOXRUN, IUCS-CESPU), 4585-116 Gandra, Portugal
[3] Polícia Judiciária, Crime Scene Investigation Department – Northern Branch, 4200-096 Porto, Portugal

* Correspondence: a35552@alunos.cespu.pt

Abstract

Background: Fingerprints (FP) recognition has gained popularity due to its wide range of applications, from unlocking smartphones to border control systems [1,2]. However, the increasing use of FP also makes them attractive targets for malicious actors, who seek develop methods to compromise FP recognition systems. One of the main threats to these systems is spoofing attacks [1]. **Objective:** Analyse reported cases of FP spoofing, highlighting their occurrence and potential misuse. **Methods:** For this review we followed the PICO framework and PRISMA guidelines. Several studies and reports retrieved from IEEE Xplore, J-Stage, and International Journal of Computer Applications were analysed. Terms like "fingerprint" AND "spoof" OR "attack" were used. Articles older than 15 years, duplicates, editorials, and reviews were excluded. Studies that reported any real-life spoofing case were included. **Results:** Several real-world cases illustrate the practical feasibility of FP spoofing and its associated risks. In 2008, the Chaos Computer Club successfully lifted the latent FP of a German minister from a glass he used and utilized it to produce 4000 plastic spoofs [3]. In 2013, the same organisation further demonstrated the vulnerability of FP systems by recreating a FP from a high-resolution photograph and generating a functional spoof using wood glue [4]. In another case reported in 2013, a medical doctor used silicone-based spoofs to fraudulently register coworkers' attendance, thereby bypassing the biometric system of a hospital in São Paulo [1,4]. In 2014, a hacker reproduced the FP of a German politician from photographs and successfully used the fabricated FP to unlock a smartphone [2]. The analysis of these cases highlights a significant gap in the literature, namely the limited availability of detailed case reports on fingerprint spoofing, which hinders systematic research and the development of effective countermeasures. Moreover, these cases consistently demonstrate the capability of spoof to bypass existing biometric security systems. **Conclusions:** This review highlights the risks associated with the unintended exposure of FP, reinforcing the urgent need for robust protective measures, particularly in commonly used devices. Furthermore, it underscores the importance of systematic reporting of spoofing incidents, since increased documentation is essential to raise awareness, support scientific research, and guide the development of effective countermeasures.

Keywords: fingerprint recreation; illicit use; spoof attacks

Acknowledgments/Funding

This research was funded by the annual funding of 1H-TOXRUN of the University Institute of Health Sciences (IUCS-CESPU).

References

1. Chugh, T. et al. Fingerprint spoof detection using minutiae-based local patches. *IEEE International Joint Conference on Biometrics (IJCB)*, Denver. **2017**, pp. 581-589, doi:10.1109/BTAS.2017.8272745
2. Echizen, I. et al. BiometricJammer: Method to prevent acquisition of biometric information by surreptitious photography on fingerprints. *IEICE Transactions on Information and Systems*. **2018**, *E101D*(1), 2–12. doi:10.1587/transinf.2017MUI0001
3. Marasco, E. et al. A Look At Non-Cooperative Presentation Attacks in Fingerprint Systems. *Eighth International Conference on Image Processing Theory, Tools and Applications (IPTA)* **2018**, pp. 1-6, doi: 10.1109/IPTA.2018.8608133
4. Chugh, T. et al. Fingerprint spoof buster: Use of minutiae-centered patches. *IEEE Transactions on Information Forensics and Security*, **2018**, *13*(9), 2190–2202. doi:10.1109/TIFS.2018.2812193