B

Biometrics Security

Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia
Universidad Autonoma de Madrid, Madrid, Spain

Synonyms

Biometrics attacks; Biometrics vulnerabilities

Definitions

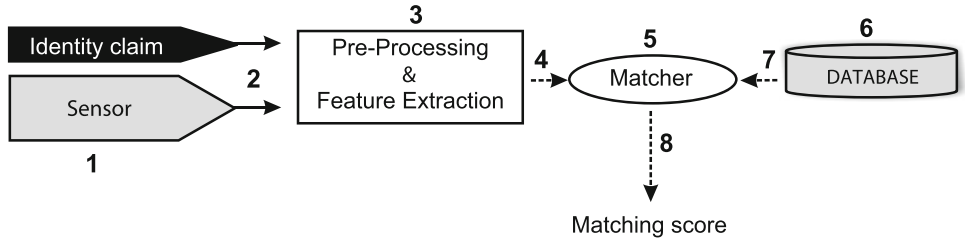
Biometrics security deals with the technologies and practice around evaluating the impact of attacks to biometrics systems and ways to countermeasure such attacks.

Application

Biometric systems can offer several advantages over classical security methods based on something that you know (e.g., PIN, password) or something that you have (e.g., key, card, ID). Traditional authentication systems are not prepared to discriminate between impostors who have illegally acquired the privileges to access a system and the genuine user. Furthermore, in biometric systems, there is no need for the user to remember difficult PIN codes that could be easily forgotten or to carry a key that could be lost or stolen. However, despite these advantages, biometric systems have some drawbacks (Jain et al. 2016), including (1) the lack of secrecy (e.g., everybody knows our face or could get our fingerprints) and (2) the fact that a biometric trait cannot be replaced (if we forget a password, we can easily generate a new one, but no new fingerprint can be generated if an impostor steals it). Furthermore, biometric systems are vulnerable to external attacks which could decrease their level of security. Basically, there are eight different points of attack on biometric recognition systems, which are depicted in Fig. 1. These **vulnerability points** can broadly be divided into two main groups (Galbally et al. 2007):

- *Direct attacks* (also known as presentation attacks or spoofing attacks (Hadid et al. 2015; Marcel et al. 2019).) One can generate synthetic biometric samples (for instance, speech, fingerprints, or face images) in order to fraudulently access a system. This is the first vulnerability point in a biometric security system (see attack point 1 in Fig. 1). These attacks at the sensor level are referred to as direct attacks. It is worth noting that in this type of attacks, no specific knowledge about the system operation is needed (e.g., matching algorithm used, feature extraction, feature vector format). Furthermore, the attack is carried out in the analog domain, outside the digital limits of the system, so the digital protection mech-

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1603-1



Biometrics Security, Fig. 1 Architecture of an automated biometric verification system. Possible attack points are numbered from 1 to 8

anisms (e.g., digital signature, watermarking) cannot be directly used.

- *Indirect attacks.* This group includes all the remaining seven points of attack identified in Fig. 1. Attacks 3 and 5 might be carried out using a Trojan horse that bypasses the feature extractor and the matcher, respectively. In attack 6, the system database is manipulated (a template is changed, added, or deleted) in order to gain access to the application. The remaining points of attack (2, 4, 7, and 8) are thought to exploit possible weak points in the communication channels of the system, extracting, adding, or changing information from them. In opposition to direct attacks, in this case the intruder needs to have some information about the inner working of the recognition system, and, in most cases, physical access to some of the application components (feature extractor, matcher, or database) is required.

In order to improve the performance and robustness of biometric systems against the mentioned potential attacks, it is of great importance to study the behavior of existing systems against those potential attacks. This has been an intense research effort in the last decade (Marcel et al. 2019).

On the other hand, several countermeasures have been developed for **securing biometric systems** against those potential attacks. The countermeasures can be classified as follows:

- *Presentation attack detection* (also known as biometric anti-spoofing or biometric fake detection (Hadid et al. 2015; Marcel et al. 2019).) Against attacking point 1 in Fig. 1, there are several techniques specifically developed for biometric systems to detect the naturalness of the input biometric in order to detect fake or manipulated biometric inputs (Galbally et al. 2014).
- *Template protection.* In order to protect attacking points 6 and 7 in Fig. 1, there are several techniques developed specifically for biometric systems that protect the biometric templates generated in the enrollment and operation of the systems. These techniques are commonly known as biometric template protection (Rathgeb and Uhl 2011; Gomez-Barrero et al. 2017a).
- *General computer security schemes.* For attacking points related to communication channels and manipulation of the processing modules in Fig. 1, one can use general computer security schemes.

Open Problems and Future Directions

Biometric template protection technologies are now evolving to improve the security of biometric systems while not harming operational aspects of those systems. Future directions in this way include incorporating into biometric systems recent advances in cryptography and distributed security like homomorphic encryption (Gomez-Barrero et al. 2017b) and blockchain technologies (Delgado-Mohatar et al. 2019).

On the other hand, the easiness to generate high-quality biometric fake and manipulated content is growing significantly nowadays with

the explosion of deep learning technologies. DeepFakes can now be created in several biometric modalities (facial images and video, voice, etc.) imitating natural biometric content in a way almost undistinguishable to the human eye (Tolosana et al. 2020). New techniques are being developed specifically to countermeasure such high-quality biometric fakes generated with deep learning technologies (Neves et al. 2020).

Acknowledgments This work has been supported by projects BIBECA (RTI2018-101248-B-I00 MINECO/FEDER), TRESPASS-ETN (MSCA-ITN-2019-860813), and PRIMA (MSCA-ITN-2019-860315).

References

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 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, CVPRW

Galbally J, Fierrez J, Ortega-Garcia J (2007) Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. In: Proceedings of Spanish Workshop on Biometrics

Galbally J, Marcel S, Fierrez J (2014) Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition. IEEE Trans Image Process 23(2):710–724

Gomez-Barrero M, Galbally J, Morales A, Fierrez J (2017a) Privacy-preserving comparison of variable-length data with application to biometric template protection. IEEE Access 5:8606–8619

Gomez-Barrero M, Maiorana E, Galbally J, Campisi P, Fierrez J (2017b) Multi-biometric template protection based on homomorphic encryption. Pattern Recogn 67:149–163

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

Jain AK, Nandakumar K, Ross A (2016) 50 years of biometric research: accomplishments, challenges, and opportunities. Pattern Recogn Lett 79:80–105

Marcel S, Nixon M, Fierrez J, Evans N (2019) Handbook of biometric anti-spoofing, 2nd edn. Springer, Cham

Neves JC, Tolosana R, Vera-Rodriguez R, Lopes V, Proenca H, Fierrez J (2020) GANprintR: improved fakes and evaluation of the state of the art in face manipulation detection. IEEE J Sel Topics Signal Process 14(5):1038–1048

Rathgeb C, Uhl A (2011) A survey on biometric cryptosystems and cancelable biometrics. EURASIP J Inf Secur 2011:3

Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J (2020) Deepfakes and beyond: a survey of face manipulation and fake detection. Inf Fusion 64:131–148