Privacy Protection of Biometric Templates

Moazzam Butt, Olaf Henniger, Alexander Nouak, and Arjan Kuijper

Fraunhofer Institute for Computer Graphics Research IGD
Fraunhoferstr. 5, D-64283 Darmstadt, Germany
{moazzam.butt,olaf.henniger,
alexander.nouak,arjan.kuijper}@igd.fraunhofer.de

Abstract. Although many biometric characteristics are not secrets, biometric reference data (also known as biometric templates) need to be stored securely and to be protected against unauthorized use. For this purpose, biometric template protection techniques have been developed that do not only prevent privacy leakage and provide confidentiality of the stored biometric templates, but address also problems like identity theft and cross-matching of biometric templates stored in different systems. This paper describes the security and privacy risks associated with storing biometric data and highlights the necessity of using biometric template protection as a potential remedy to these risks. Privacy considerations are discussed with respect to using fingerprint verification for access control to a public outdoor swimming pool.

1 Introduction

Biometrics, i.e. the automated recognition of individuals based on their biological and behavioural characteristics, is a promising technology for automating user authentication at human-machine interfaces. Common biometric modalities used at human-machine interfaces nowadays are face, fingerprint, iris, vein pattern, voice, handwritten signature, or gait. Biometric authentication methods provide convenience to the users and enhance the binding of the authentication process to persons provided that their recognition accuracy and resistance against fraud are sufficiently high. An increase in the deployment of biometric systems is observed in the civil domain (such as UIDAI Aadhaar [1], US-VISIT programmes [2]) and in the forensic domain (such as AFIS). On the other side, security and privacy fears like personal data misuse or hacking, mass surveillance, personal data peering or sharing via centralised storage in the cloud and cloud-based services have become major concerns these days. Hence, use of biometrics in systems needs to preserve privacy by design and must not violate the human right to privacy and freedom from surveillance.

The remainder of this paper is organized as follows: Section 2 describes the general flow of information and vulnerabilities in biometric systems. Section 3 gives an overview of biometric template protection. Section 4 discusses the concerns raised by a recent practical deployment experience at a public outdoor swimming pool in Germany. Section 5 comprehends the conclusions.

C. Stephanidis (Ed.): HCII 2014 Posters, Part I, CCIS 434, pp. 153–158, 2014.

2 Privacy and Security in Biometrics

Fig. 1 illustrates the general flow of information within a biometric system: Biometric samples are acquired from a subject via a sensor. The sensor output is sent to a processor that extracts distinctive, repeatable biometric features. The resulting features can be stored in the biometric enrolment database as a biometric template. In some cases, the captured biometric data themselves (without prior feature extraction) are stored as reference. A probe biometric sample can be compared to a specific reference, to many references, or to all references in the enrolment database to determine if there is a match. A decision regarding acceptance or rejection is taken based upon the similarity between the features of the probe and those of the references compared. Fig. 1 also identifies potential points of attack within a biometric system.

A main threat to a biometric system is that of impersonation, i.e. of an impostor masquerading as another person who is enrolled and gaining access to the protected assets. The success rate of zero-effort impostor attacks (in which an impostor presents the own biometric characteristics in order to get falsely accepted as somebody else's biometric look-alike) is related to the system's false accept rate. If unwatched, an impostor may also attempt to impersonate an enrolled person by use of a dummy such as a silicone or gummy finger or a reproducing device such as a voice recorder.

Although many biometric characteristics are not secrets (e.g., anyone can rather easily take photographs of someone else's face), biometric data are considered personal data as defined in [3]. Personal data is required to be stored securely and to be used in a privacy preserved manner [4]. Unlike the ubiquitous passwords, biometric templates can only a limited number of times be replaced with different biometric traits of the same person due to limited availability (only one face, two eyes, ten fingers, etc.). Furthermore, they do not only contain information about biometric features of a person, but may also contain personal information beyond what is needed for authentication. For instance, information about gender, ethnic origin, body conditions and diseases, which one may like to keep private, can be inherently attached to a face template. Because biometric data are highly sensitive personal data, many people are troubled by the risks associated with storing biometric templates in computer systems [5,6,7,8].

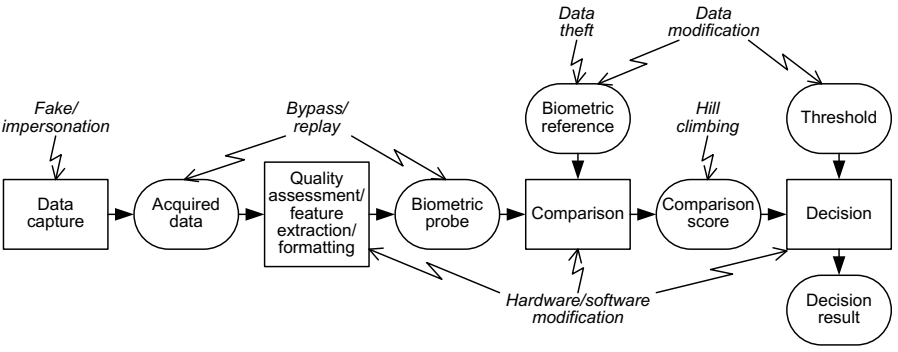

Fig. 1. Examples of attacks against a biometric system

Biometric template protection is not only needed for privacy preservation, but also for protecting against identity theft and other attacks. Cross-matching attacks could allow an impostor, who gets hold of the biometric reference of another person stored in one system, to intrude all other systems where the same biometric reference is used. A stolen biometric template must not be usable as a blueprint for biometric presentation attacks, e.g. for the generation of an artificial gummy fingerprint (spoofing).

Also other vulnerable points indicated in Fig. 1 may be attacked to gain access to protected assets. For instance, if bypass and replay attacks are possible, an impostor could send recorded or otherwise acquired biometric data to the comparison component, evading the regular data capture device. If comparison scores are revealed, an impostor could systematically modify biometric probes in a hill-climbing attack to obtain comparison scores closer and closer to the decision threshold until the threshold is met. There are long-established standards and best practices for ensuring IT security that must be applied also to protect biometric systems.

3 Biometric Template Protection

The confidentiality of stored passwords is usually protected by cryptographic hash functions. The hash value of a presented password must match bit by bit the stored hash value. This approach cannot be applied directly to biometric data because the biometric data captured from the same person are never completely the same due to their natural variability. Using general-purpose cryptographic algorithms for encrypting the stored biometric references is also not a satisfying solution because encrypted biometric data must be decrypted for comparison with the claimer's data, which makes them vulnerable to attacks at the comparison stage.

One of the solutions to cope with the threats to biometric templates is to store and to compare biometric data in tamper-proof smart cards. However, smart-card based systems are not always applicable.

For the protection of biometric templates in an insecure environment, special biometric template protection techniques have been developed. Biometric template protection techniques generate binary templates that can be used for biometric authentication and at the same time preserve privacy. It is computationally hard to retrieve the original biometric characteristic or any personal or private information attached to it from these binary templates. For that reason, they are called protected biometric templates or pseudonymous identifiers (PI) [9].

Biometric template protection techniques do not only prevent privacy leakage, but also resolve the risk of cross-matching by allowing to generate multiple templates that are statistically independent from each other. The number of templates that can be generated depends on the entropy of the biometric modality. These templates can be stored in different biometric application servers for personalizing different services. Multiple templates, extracted from a single biometric sample, also offer revocability (or cancelability), i.e., a new biometric template can be assigned if a template is compromised.

Biometric template protection techniques must also not lead to a significant degradation of the recognition accuracy, i.e. of the false reject rate and false accept rate, of a biometric system.

Several biometric template protection techniques have been proposed under a unified architecture [9]. These techniques can be categorized into two types, biometric cryptosystems and feature transformation [10]:

- Biometric cryptosystems have been developed utilizing cryptographic primitives. In these schemes, either a consistent key is generated from the biometric sample (key generating biometric cryptosystems) or a bound cryptographic key is released (key binding biometric cryptosystems) provided the error correction coding [11] can overcome the difference between the biometric probe and the samples given at enrolment. In order to overcome the intra-class variance between the biometric samples at the enrolment and authentication stages, helper data (also called auxiliary data [9]) is stored in addition to the protected biometric template. At the authentication stage, this helper data is used for error correction. Key binding biometric cryptosystems lead to a binary match/non-match decision. Hence, there is no possibility that an adversary could exploit comparison scores to regenerate biometric templates in an iterative fashion in a hill-climbing attack [6].
- Feature transformation methods transform the biometric features extracted from the original biometric sample using a non-invertible transformation [12,13] or a user-specific invertible transformation (salting) [14]. These techniques inherently support template diversity and revocability as changes in transformation parameters may result very conveniently in many new templates from one single biometric sample. The challenge is to design a transformation that is irreversible and robust to intra-class variance [15]. The transformed data may or may not have the same domain as the original data [12]. The comparison takes place using distance measures resulting into a score. The score is compared with a pre-adjusted threshold resulting in a match/non-match decision. In salting-based approaches, the transformation parameters are derived from a user password. In this case, the security of the protected biometric template is tied to the security of the user password [16,17].

4 Use Case: Access Control to Public Outdoor Pool

In the following, we discuss a deployment scenario of using biometrics for access control to a public outdoor swimming pool in Germany. The pool entrance was originally operated by staff and the ticket to the pool was not personalized, i.e. no information about the holder was printed on the ticket. The motivation for using biometrics here was to bind the season tickets to their holders and to prevent sharing the same season ticket between several persons by providing a mechanism of identity verification. Season-ticket holders received RFID chip cards (Mifare) with stored encrypted fingerprints, and a RFID reader with integrated fingerprint sensor was installed at the pool entrance. To enter the pool, the user had to first touch the card on the RFID reader in order to upload the fingerprint template to the reader. As next step, the user gave his fingerprint and the access-control terminal compared the template with the live scan. In case the probe sample matched the template, the gate was opened; otherwise not. The advantage of storing the fingerprint template on a card is that the reference template is always in the custody of the user. The use of fingerprints for access-control to the pool was all voluntarily, i.e. the users signed declarations of consent.

However, after petitions from citizens who did not accept being fingerprinted for accessing a public swimming pool, the regional data protection authority complained about the above scenario [18]. The data protection authority considered the use of fingerprints objectionable because of

- lack of an equivalent alternative (holders of season tickets without fingerprint had to wait for the pool attendant to open the entrance door) and
- disproportionality of using fingerprints in local-government services for the public.

As a result, the use of biometrics for access-control was abandoned. This resulted in termination of the option of season tickets (allowing any number of entries during a season). The RFID chip cards are now used as rechargeable payment cards at an unstaffed access-control terminal instead.

This example suggests that the use of biometrics for local government services for the public is far from certain although methods of biometric template protection already exist. In private-sector recreation facilities (fitness clubs etc.), biometrics may still be used on a voluntarily basis, provided that biometric template protection schemes are deployed. A lesson learnt is that there must be an equivalent alternative for people who do not accept using biometrics. The use-case scenario also highlights the need to raise awareness of the potential of biometric template protection techniques.

5 Conclusions

The use of biometric data for public-domain applications is subject to EU data privacy regulations [3,4]. Often, the use of biometric data is perceived to bring less added value than added privacy and security risks even if being convenient for citizens.

Central storage of biometric references is susceptible to cyber-attacks and misuse of personal data. Smart cards can be used as an alternative to central storage. In this way, access to a biometric template and demographic data associated with it remains limited and, hence, also protected from many external attacks described in Section 2. Moreover, the personal data can always be used only on a voluntary basis, and the data remains at the disposal of the actual owner. Smart cards can also provide a tamper-proof platform for biometric comparison on card [19]. Nowadays, smartphones can replace smart cards and, therefore, a dedicated separate hardware token is not necessary. New technologies like near-field communication (NFC) can make the transmission of biometric data feasible and interoperable.

Irreversible biometric templates created by biometric template protection techniques can aid in overcoming the issue of proportionality. The development of certifiably secure and privacy-enhancing biometric systems will increase the level of trust in biometric systems. Methods for assessing the privacy and security properties of the biometric template protection techniques have already been investigated e.g. in [20].

Acknowledgement. This work has received funding from the European Community's Framework Programme (FP7/2007-2013) FIDELITY project under grant agreement no. 284862.

References

1. Unique Identification Authority of India. AADHAR, http://uidai.gov/in
2. US Department of Homeland Security, http://www.dhs.gov/us-visit-traveler-information
3. European Parliament, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (october 1995), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
4. European Convention on Human Rights (December 1950), http://www.echr.coe.int/Pages/home.aspx?p=press/factsheets&c=
5. Hill, C.: Risk of masquerade arising from the storage of biometrics, B.S. thesis, Australian National Univ., Canberra, Australia (2013), http://chris.fornax.net/biometrics.html
6. Adler, A.: Vulnerabilities in biometric encryption systems. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 1100–1109. Springer, Heidelberg (2005)
7. Mohanty, P., Sarkar, S., Kasturi, R.: Privacy and security issues related to match scores. In: Proc. Conf. Computer Vision and Pattern Recognition Workshop, pp. 162–165 (2006)
8. Jain, A.K., Bolle, R., Pankanti, S. (eds.): Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers (1999)
9. ISO/IEC, ISO/IEC 24745 Information technology - Security techniques - Biometric information protection, ISO/IEC JTC 1/SC 27 (2010)
10. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, 1–20 (January 2008)
11. Hall, J.I.: Generalized Reed-Solomon codes. Notes on Coding Theory, 63–76 (2003)
12. Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometric-based authentication systems. IBM Syst. J. 40(3), 614–634 (2001)
13. Teoh, A., Goh, A., Ngo, D.: Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Trans. Pattern Anal. Mach. Intell. 28(12), 1892–1901 (2006)
14. Ngo, D., Teoh, A., Goh, A.: Biometric hash: High-confidence face recognition. IEEE Trans. Circuits Syst. Video Technol. 16(6), 771–775 (2006)
15. Sutcu, Y., Sencar, H., Memon, N.: A secure biometric authentication scheme based on robust hashing. In: Proc. Seventh Workshop Multimedia and Security, pp. 111–116 (2005)
16. Teoh, A.B.J., Connie, T., Ngo, D., Ling, C.: Remarks on biohash and its mathematical foundation. Inf. Process. Lett. 100(4), 145–150 (2006)
17. Lumini, A., Nanni, L.: An improved biohashing for human authentication. Pattern Recognition 40(3), 1057–1065 (2007)
18. Ronellenfitsch, M.: 40. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten (2011)
19. Eurosmart, Smart biometrics for trust and convenience – Analysis of use cases and best practice recommendations, Eurosmart Reference Paper (April 2012)
20. Zhou, X.: Privacy and security assessment of biometric template protection, PhD thesis, TU Darmstadt (2011)