Biometric Privacy Protection: Guidelines and Technologies

Ruggero Donida Labati, Vincenzo Piuri, and Fabio Scotti

Università degli Studi di Milano, Department of Information Technology,
via Bramante 65, I-26013 Crema (CR), Italy
{ruggero.donida,vincenzo.piuri,fabio.scotti}@unimi.it
http://www.dti.unimi.it

Abstract. Compared with traditional techniques used to establish the identity of a person, biometric systems offer a greater confidence level that the authenticated individual is not impersonated by someone else. However, it is necessary to consider different privacy and security aspects in order to prevent possible thefts and misuses of biometric data. The effective protection of the privacy must encompass different aspects, such as the perceived and real risks pertaining to the users, the specificity of the application, the adoption of correct policies, and data protection methods as well. This chapter focuses on the most important privacy issues related to the use of biometrics, it presents actual guidelines for the implementation of privacy-protective biometric systems, and proposes a discussion of the methods for the protection of biometric data.

Keywords: Biometrics - Privacy - Security - Template protection.

1 Introduction

Traditional techniques used to establish the identity of a person are based on surrogate representations of his/her identity, such as passwords, keys, tokens, and identity cards. In many situations, these representations cannot guarantee a sufficient level of security because they can be shared, misplaced or stolen. Biometric recognition systems, instead, are based on physiological or behavioral characteristics of the individual, which are univocally related to their owner, cannot be shared or misplaced, and are more difficult to be stolen. The use of biometric systems is continuously increasing in different applicative scenarios [46] and the related market is showing a significant positive trend. In 2011, it reached the amount of 5 billion dollars and it is expected to reach 12 billion dollars by the end of 2015 [1]. Typical applicative scenarios are: physical access control (critical areas, public buildings, sport arenas, bank caveau, transportations, etc.); surveillance (private buildings, public areas, etc.); government applications (identity cards, passports, driving licenses, immigration control, health cards, access control to online government services, etc.); forensic applications (body identification, crime investigation, searching of disappeared childrens, kinships, intelligence, etc.); logical access control to data, networks and services (home banking, ATM, supermarkets, e-commerce, mobile phones, computers, etc.).

In order to prevent possible thefts and misuses of biometric data, it is necessary to consider different privacy and security aspects. Security and privacy are two different concepts because the privacy protection is more restrictive than the security protection. The security ensures: authentication, data integrity, confidentiality, and non-repudiation. Differently, the privacy requires also the data protection.

The protection from privacy abuses is very important in biometric systems. For example, if the biometric data related to an individual are stolen, this person can be impersonated for a long period of time and it is not easy to modify or substitute the compromised data. This is due to the fact that biometric traits are unique for each individual and strictly associated to their owner. Moreover, biometric traits are irrevocable, in the sense that the association cannot be changed during the human life.

The public acceptance of a biometric system is strictly related to the privacy risks perceived by the users. Usually, these risks are different from the real risks associated to a biometric system. In general, the most important perceived risk is related to possible identity thefts. Other perceived risks are related to misuses of the personal data, for example for tracing all the activities of the individuals or for operating proscription lists. Real risks should be evaluated considering different factors associated to the applicative context and used biometric traits. Examples of these aspects are the modalities adopted for storing the personal data, the owner of the system, the used recognition modality (authentication or identification in a biometric database), the durability of the used traits, and the class of the trait (physiological or compartmental).

It is possible to consider a privacy-protective biometric system as a system that drastically reduce the real risks associated to the use of biometric data. In order to properly design a privacy-protective biometric system, it is not sufficient to evaluate only aspects related to performances, costs, acceptability, and applicative conditions, but it is necessary to follow a set of guidelines for the use of biometric data [32]. These guidelines permit to effectively reduce the risks related to possible misuses of personal data.

In order to protect the privacy of the users, it is also necessary to consider the possible attacks that can be performed to a biometric system. In general, biometric systems are composed by four modules: sensor, feature extractor, database, and matcher. Each module can be subject to adversary attacks. As shown in Fig. 1, it is possible to distinguish eight distinct classes of attacks to the different modules [19, 44, 47]: (I) fake biometric at the sensor, (II) resubmission of old digitally stored biometrics signal, (III) override feature extractor, (IV) tampering with the feature representation; (V) override matcher, (VI) tampering with stored templates, (VII) channel attack between stored templates and the matcher, (VIII) decision override.

There are different classes of techniques that should be used to protect the privacy of the users also from possible attacks. Every component of the biomet-

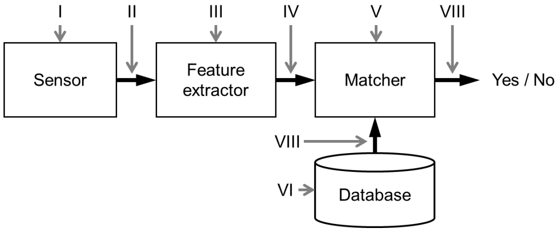

Fig. 1. Points of attack in a biometric system.

ric system should in fact be protected by using properly methods. Important classes of techniques are: liveness detection methods, physical and cryptographic methods for the channel protection, secure code execution practices, template protection methods [25].

In this chapter, the most treated class of techniques for the protection of biometric systems regards the template protection methods. In a biometric application, the template is an abstract representation of the physiological or behavioral features, extracted from the acquired biometric samples (signals, images, or frame sequences). Template protection methods permit to perform the recognition by using a protected representation of the biometric templates. In the literature, there are different methods for the biometric template protection: methods based on the transformation of the template (cancelable biometrics), methods based on cryptographic algorithms that perform the recognition by comparing cryptographic keys (biometric cryptosystems), methods based on cryptographic techniques that permits to perform a set of operations without converting the data in the plain domain (cryptographically secure methods).

The chapter discusses the privacy issues related to the use of biometrics and presents some of the most advanced techniques available today for the privacy protection of biometric data. Section 2 presents the problems related to the privacy risks, describes a possible classification of the privacy protection levels, and overviews the guidelines for the design of privacy-protective biometric systems. Section 3 proposes a brief review of the template protection techniques in the literature, while the last section is devoted to conclusions.

2 Privacy in Biometric Systems

Traditional authentication methods are based on somewhat known (e.g. a password) or a possessed object (e.g. a key or a token). If passwords or keys are theft of stolen, it is easy to revoke or replace them. Differently, biometric traits are univocally related to their owners and cannot be replaced or modified. If data related to a biometric trait are stolen, the owner of the trait can be impersonated in many different biometric systems and for a long period of time or the individual can be included in different biometric systems without explicit consents. For this reason, it is particularly important to protect biometric data.

It is possible to distinguish three different perspectives about the privacy in biometrics. The first perspective is related to the risks perceived by the users and should be considered in order to evaluate the acceptability of the system itself. The second perspective regards the application context in which the biometric system should be exploited and permits to properly design privacy protection techniques. The last aspect that should be considered is the used biometric trait. Each biometric trait, in fact, presents different propriets.

The evaluation of the risks perceived by users is a complex task because the risk perception is different for every person. Generally speaking, one of the most important perceived risks is related to the fact that the persons consider the acquisition of the biometric traits as an exact permanent filing of their activities and behaviors, and the idea that the biometric systems can guarantee a recognition accuracy equal to 100% is very common. Other perceived risks consist in the use of the collected biometric data for malicious purposes, and for tracing all the activities of the individuals or for operating proscription lists. Another important perceived risk is the fact that the acquisition of some biometric traits can be dangerous for the health. For example, the iris images are usually captured by using infrared illuminators, which can be erroneously considered as harmful). This psychological aspects should been taken into account, and, during the deployment of the biometric system, it is very important to inform the users about the real risks for the health and for the privacy, as well as all the procedures designed and applied to protect the biometric data.

The evaluation of the application context permits to determine some real risks of privacy invasiveness. Table 1 plots a qualitative representation of the privacy risks versus ten different application features, according to the International Biometric Group [32]:

1. *Covert* recognition systems (for example surveillance applications) are more privacy invasive than *overt* biometric systems. In some cases, covert applications can use biometric data without any knowledge or explicit consent of the individuals.
2. Applications that require a *mandatory* use of biometric systems are more invasive for the user's privacy than applications in which the use of biometric technologies is *optional*. In this case, the users can decide to not be checked by a biometric system, and they can adopt a different authentication method.
3. *Identification* systems perform the biometric recognition by comparing the acquired biometric data with N identities stored in a database. *Authentication* systems consider only the acquired biometric data and the declared identity, performing a 1 to 1 comparison. In most of the cases, the biometric database used for performing the identification is situated in a physical place different from the one in which the biometric sensors is located. For these reasons, identifications present more privacy risks than authentications.
4. It is possible to distinguish systems that use biometric data for a *fixed period* and systems that can use these information for *indefinite* time. Policies that define the storing duration of biometric data can reduce privacy risks.

Table 1. Applicative aspects concerning the privacy according to the IBG (Iternational Biometric Group).

Lower Risk	Question	Greater Risk
Overt	Is the system deployed overtly or covertly?	Covert
Optional	Is the system optional or mandatory?	Mandatory
Verification	Is the system used for Identification or Verification?	Identification
Fixed Period	Is the system deployed for a fixed period of time?	Indefinite
Private Sector	Is the system deployed in the private or public sector?	Public Sector
Individual/Customer	In what role is the user interacting with the system?	Employee/Citizen
Enrollee	Who owns the biometric information?	Institution
Personal storage	Where is the biometric data stored?	Database Storage
Behavioral	What type of biometric technology is being deployed?	Physiological
Templates	Does the system use templates, samples or both?	Sample/Images

5. Usually, biometric applications in the *public sector* are considered to be more susceptible to privacy invasiveness than applications in the *private sector*. An important fear of the users is related to possible government abuses.
6. The role of the individuals that use the biometric system has great impact on the privacy. The privacy risks are associated to the rights of the individuals over the stored biometric data, and are lower in the case when the users retain usage rights. For example, there are more privacy risks for *employees and citizens* than *individuals and costumers*.
7. The applications in which private or public *institutions* own the used biometric data are more privacy invasive than the applications in which the users (*enrollee*) own their data. The user control of the data is not possible in all the biometric applications.
8. Biometric systems that use databases of biometric data (*database storage*) present more privacy risks with respect to systems based on data stored in smartcard or memory devices possessed by the users (*personal storage*) because the use of personal memory devices can prevent possible abuses.
9. The use of *physiological* biometric traits presents more privacy risks than the use of *behavioral* traits. In most of the cases, physiological traits can obtain more recognition accuracy, are more harder to mask or alter, and can be acquired with less user cooperation.
10. Biometric systems that store *samples and images* are more subject to privacy risks than systems that store biometric *templates*. This is due to the fact that templates reveal more limited information.

In order to determine the real risks of privacy invasiveness, it is also necessary to consider the adopted biometric traits because they can introduce different kinds of risks. Four important features related to the tecnologies associated to the different biometric traits are presented in [32]:

1. The first feature is the possibility to use the biometric trait in *identification* systems. Not all the biometric traits can be used for the identification because this process requires high performances in terms of accuracy and speed. Examples of biometric traits that can be used for performing the

identification are the iris and fingerprint. In general, systems based on traits that can be used in identification are more invasive for the user's privacy.

2. The second feature is associated to the possibility of the trait to be used in *covert* systems. For example, the face trait can be more easily used in covert recognition systems with respect to the fingerprint trait. Covert systems present more privacy risks than overt systems.
3. The third feature evaluates how much biometric traits can be considered as *physiological or behavioral*. Not all the biometric traits can be considered as completely physiological or behavioral. The face trait, for example, can be considered as physiological but can be modified by the user's behaviors (expressions, make up, etc.). Behavioral traits can be considered as more privacy compliant because they can be modified by the users and are less permanent then physiological traits.
4. The forth feature is the *database compatibility* and is related to two points: the technology interoperability between systems based on different databases, and the presence of numerous and/or large biometric databases. An example of trait with high database interoperability is the fingerprint since there are many large databases containing standardized templates related to this trait. Traits characterized by a lower technology interoperability can be considered as more privacy compliant.

Performing a weighted mean of these features, it is possible to classify the overall risk level related to the technologies based on a specific biometric trait. Examples of traits that present a high risk level are the face and fingerprint. A medium risk can be assigned to the iris and retina, and traits characterized by low risks for the privacy are the hand, voice, keystroke, and signature.

Considering the different characteristics of the traits and application contexts, the development and deployment of biometric systems requires the analysis of at least nine different aspects: cost, usability, speed, social acceptance, accuracy, scalability, interoperability, security, and privacy. Different biometric technologies can provide good performances in one or more of these aspects. The choice of the adopted technology should be done by considering the most import characteristics for the evaluated application. As shown in Fig. 2, the nine main evaluative aspects can be quantized and plotted in a nine-dimensional space (e.g., in a spider diagram), where a specific application is represented by a point in this space.

Considering the privacy aspect, it is possible to define four different classes: protective, sympathetic, neutral, invasive [32]:

1. *Privacy-protective applications* use biometrics in order to protect personal information that might otherwise be compromised. In this case, the use of biometric recognition techniques provide a mean for an individual to establish a trusted identity, and permits to limit the accesses to sensible data. Examples of privacy-protective applications are systems for the enterprise security and accountholder verification:
2. *Privacy-sympathetic applications* are designed to protect the biometric data from unauthorized access and usage. All the elements of these applications

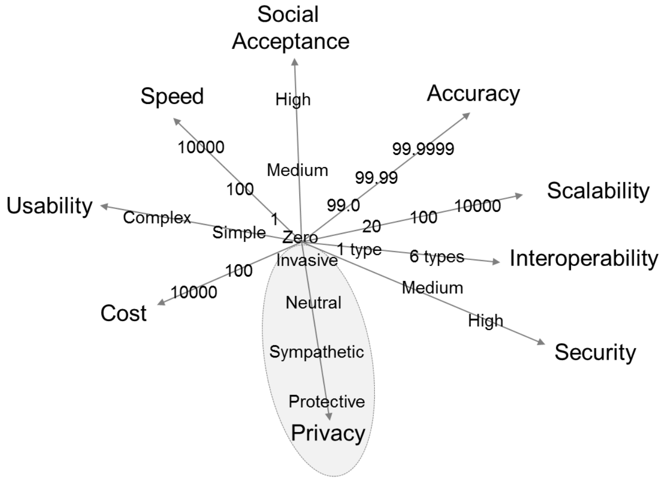

Fig. 2. Evaluative aspects of biometric systems.

are designed considering privacy protection techniques. Most of the current applications can incorporate privacy-sympathetic elements.

3. *Privacy-neutral applications* use biometrics without considering privacy aspects. In these applications, the privacy impact is usually slight. Examples of privacy-neutral applications are some access control technologies and authentication systems for electronic devices (personal computers, mobile phones, etc.).
4. A *Privacy-invasive applications* permit the use of personal data in a fashion that is contrary to privacy principles. Applications that use biometrics without any knowledge or explicit consent of the individuals and systems that use biometric data for undisclosed purposes or beyond the initial scope appertain to this class. Surveillance applications and some national ID services can be considered as privacy-invasive.

In order to design privacy-sympathetic and privacy-protective systems, it is necessary to follow a set of guidelines [32]. These guidelines are related to: scope and capabilities of the system; user control of personal data; disclosure, auditing and accountability of the biometric system; data protection techniques:

1. The *scope and capabilities* of the system should be declared to the users and should not be extended during the life of the system. Biometric data should also be deleted from the database after a period of time known by the users. The storage of biometric data is particularly critical. In order to protect the privacy of the individuals, in fact, it is necessary to store only the minimum quantity of information necessary to perform the biometric recognition. For this reason, no other data should be saved and the system should store only biometric templates deleting raw data (images, signals,

and frame sequences) as soon as possible. Moreover, no other personal data should be integrated into the biometric template biometric templates should not be used as unique identifiers.

2. The user should have the *control* of the biometric data. The use of the biometric system should be voluntary. The user should also have the possibilities to be unrolled and to change or modify her data. Users should also be enrolled with some degrees of anonymity.
3. A *disclosure* regarding the biometric system should be provided. This document should regard the system purpose, enrollment modalities, matching modalities, optional or mandatory use of the biometric recognition, individuals who are responsible for the system, the data protection system. In fact, it is important to let users know when the biometric system is used, especially when enrolment and verification or identification phases are carried on. Each operator should also be made *accountable* in order to detect possible errors or misuses. Moreover, the owner of the biometric system and the operators should be to provide a clear and effective process of *auditing* when an institution or a third party entity need to perform a critical review of all the modules which compose the biometric system.
4. The system should also provide mechanisms for the *protection* of all the steps performed by the biometric system from possible attacks. Aspects that should be considered are: use of encryption primitives, adoption of private networks, design and management of algorithms and infrastructures based on the state of the art best practices, placement of the biometric system in a secure and controlled area. These aspects should be maintained throughout the life cycle of the of the system and the results of every performed recognition recognitions should also be protected. Another important practice is to limit the access to the biometric data to a defined number of operators. Template protection techniques should also be adopted in order to improve the user acceptance of the system and to overcame legal issues related to the respect of privacy protection laws that are currently ruling in several countries.

3 Technologies for Biometric Privacy

In the literature, there are many different methods for the protection of biometric templates. An ideal biometric template protection method should satisfy four properties [24, 25]:

1. *diversity:* the secure template must not allow cross-matching across databases;
2. *revocability:* compromised template can be revoked;
3. *security:* the estimation of the plain template from the secure template must be computationally hard;
4. *performance:* the accuracy of the biometric system must not be degraded by the biometric template protection method.

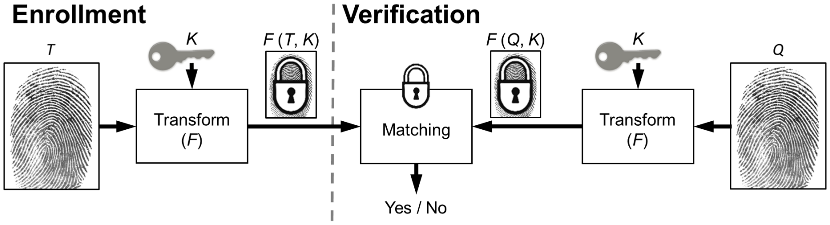

Fig. 3. Cancelable biometrics: enrollment and verification.

These four proprieties cannot be guaranteed by encrypting the templates with standard methods (e.g. RSA, AES, etc.). In fact, using these methods, the intraclass variability (biometric data captured from the same biometric trait look different from one another) does not allow to perform the matching in the encrypted domain. Therefore, it is necessary to decrypt the templates during every recognition attempt. This approach is not secure and it is necessary to adopt methods designed for the protection of biometric data.

In the literature, most of the biometric template protection methods are based on two different classes of techniques: cancelable biometrics, and biometric cryptosystems [25, 45]. Recent researches also proposed other approaches based on cryptographically secure methods [11].

3.1 Cancelable biometrics

Cancelable biometrics are based on intentional, repeatable distortions of biometric data. The used transformations permit to perform comparisons of biometric templates in the transformed domain [42]. During the enrollment phase, the biometric data T is modified by applying a transformation function F with parameters K obtained by a random key or a password. The transformed template $F(T, K)$ is then stored in the database. The authentication step applies the same transformation to the query data Q and directly matches the transformed templates $F(Q, K)$ and $F(T, K)$. Fig. 3 schematizes the described process.

The main advantage of this technique is that, if a transformed template is compromised, cancelable biometrics permit to easily substitute the stored transformed template by changing the transformation parameters. The design of the transformation functions is particularly critical because it is necessary to adopt functions that are robust to intra-class variations in order to do not reduce the accuracy of the biometric system. Another aspect that should be considered is that the correlation of transformed templates should not reveal information about the transformation function. Transformation functions can be applied to biometric samples (e.g. face images [2]), processed signals (e.g. the iris pattern [12]) or templates (e.g. features extracted from a face image [53]). It is possible to distinguish two different classes of methods: biometric salting, non-invertible transforms.

Usually, systems based on the biometric salting transform features using an invertible function defined by a user-specific key or password. Considering that the used transformation is invertible, the password must be securely stored by the user and presented during each authentication. The principal advantage of the biometric salting is that it is possible to use multiple templates for the same biometric trait because the keys are specified by the users. An important limitation of methods based on keys or passwords is that they are not usable in identification systems. Moreover, if the key is known, it is possible to obtain the original template. In the literature, one of the most used methods based on the biometric salting is the BioHashing [2, 54, 39]. This method is designed for the fingerprint trait and is divisible in two steps [27]: an invariant and discriminative transform of the biometric data, with a moderate degree offset tolerance; a discretization of the data. There are also methods designed for face recognition systems. One of these methods uses the Fisher discriminant analysis and then performs a transformation of the obtained vectors by using a randomly selected set of orthogonal directions [53]. Differently, the method proposed in [49] is based on minimum average correlation energy filters. Salting methods can also be applied to different biometric traits (e.g. iris [12], palmprint, and dynamic handwriting [36]).

In the literature, many methods secure the templates by using non-invertible transformation functions. Non-invertible transformation refers to a one-way function that is computable in polynomial time and hard to invert. The main advantage of this class of methods is that the protection of the plain biometric template is more secure than the one offered by the methods appertaining to the salting class. In fact, if the key and/or the transformed template are known, the estimation of the plain template is a computationally hard task (considering a brute force attack). Another advantage of these methods is that diversity and revocability can be achieved by using different transformation functions. The main problem is that it is difficult to design transformation functions that satisfy both the discriminability and the non-invertibility. For example, a study on the measurement of the real non-invertibility of methods based on the fingerprint is presented in [37]. Another important aspect is that the transformation function depends on the biometric features to be used in a specific application. Moreover, similarly to the biometric salting, the adoption of keys obtained by passwords or tokens does not permit to use methods based on non-invertible transformation functions in identification systems. In the literature, there are methods based on non-invertible transformation functions designed for different biometric traits. For example, fingerprint [28], face [56, 55], and signature [35]. A general schema is proposed in [42] and is based on a non-invertible function designed to transform a point pattern by using high order polynomials. This method can be used in fingerprint based on minutiae features, and voice recognition systems. Also the approach proposed in [43] is designed for fingerprint recognition systems and proposes three different functions (Cartesian, Polar, and functional) in order to transform minutiae templates. A different schema called Biotope is proposed in [6, 7]. This schema transforms the original biometric data by using crypto-

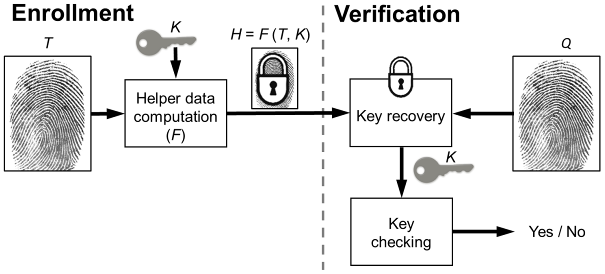

Fig. 4. Key-binding biometric cryptosystem: enrollment and verification.

graphic primitives and supports a robust distance metric in order to perform the matching. The approach supports both transforms that are public-key cryptographically invertible and/or using cryptographic one-way functions (such as MD5). The Biotope schema can be applied to different biometric traits, such as face [6] and fingerprint [7].

3.2 Biometric cryptosystems

Biometric cryptosystems was originally designed in order to secure cryptographic keys by using biometric information or to directly compute cryptographic keys from biometric data [25]. Nowadays, these techniques are also used for the privacy protection of biometric templates. Biometric cryptosystems store public data regarding the biometric trait, called helper data. During the authentication process, the helper data is used in order to extract a cryptographic key from the biometric query sample. The matching step checks the validity of the obtained key in order to verify the identity. It is possible to divide the biometric cryptosystems in two different classes: key-binding biometric cryptosystem, and key-generating biometric cryptosystem.

Key-binding biometric cryptosystems store helper data by biding the template with a chosen cryptographic key. The binding process obtains a helper data considerable as a single entity that embeds both the key and the template without revealing information about them. In fact, it is computationally hard to estimate the key or the template without knowing the user's biometric data. The authentication is performed by using the query template in order to retrieve the cryptographic key from the helper data. Usually, this task is based on error correction algorithms. If the obtained key corresponds to the correct cryptographic key, the result of the authentication is a match value. Fig. 4 shows a general schema of the key-binding biometric cryptosystem.This class of methods has two main advantages. First, the helper data does not reveal much information about the key or the biometric data. Moreover, this approach is tolerant to intra-user variations. The main limitation consists in the degradation of the accuracy of the biometric system caused by the substitution of the original matching algorithms with error correction schemes. Moreover, these methods do not guarantee diver-

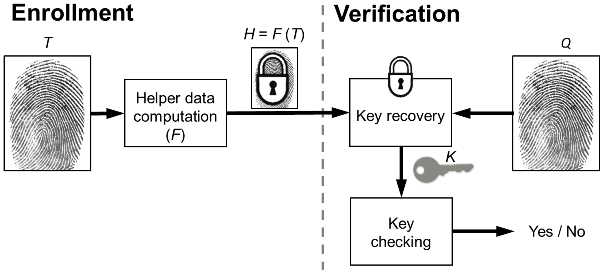

Fig. 5. Key generating biometric cryptosystem: enrollment and verification.

sity and revocability. The firstly proposed key-binding biometric cryptosystems based on fingerprints are Mytec1 and Mytec2 [40], which are based on the correlation between filter functions and the biometric images. Another well-known approach in the literature is the fuzzy commitment scheme [30]. This approach combines error correcting codes algorithms and cryptography techniques in order to achieve a cryptographic primitive called fuzzy commitment. During the enrollment, a biometric template x composed by a fixed length feature vector and a codeword w of an error correction schema C are bound. The helper data (fuzzy commitment) consists in $x - w$ and $h(w)$, where h is a hash function. The biometric matching tries to reconstruct w starting from a biometric query x'. First, the stored value $x - w$ is subtracted from x', obtaining $w' = w + \delta$, where $w' = x' - x$. If the value w is obtained by applying the error correction schema C to w', the result of the matching step is positive. The fuzzy vault [29] approach uses a set A to lock a secret key k, yielding a vault V_A. If the key k is reconstructed by using a set B that is sufficiently similar to A, the vault V_A is unlocked. This approach is based on polynomial encoding and error correction algorithms. Examples of other approaches appertaining to this class are the shielding functions [21] and distributed source coding [16]. In the literature, there are methods based on different biometric traits. For example, face [22], fingerprint [38], iris [31], and signature [33].

Key generating biometric cryptosystems compute a cryptographic key directly from the biometric data. The recognition process performed by biometric systems based on key generating biometric cryptosystems is similar to the one executed by using key-binding biometric cryptosystems but do not requires external keys. The schema of this process is shown in Fig. 5. The main advantage of these methods is that the obtained cryptographic keys can be used in many applications. However, an important problem is that it is difficult to generate keys with high stability and entropy [23, 9]. Two well-known approaches are the secure sketch and fuzzy extractor [15]. Secure sketches solve the problem of error tolerance, enabling the computation of a public key P from a biometric reading r, such as from another reading r' sufficiently close to r it is possible to reconstruct the original one. Fuzzy extractors address the problem of non-uniformity by associating a random uniform string R to the public string P still keeping all the properties of secure sketches. Indeed, fuzzy extractors can be built out of secure sketches and enable to recovering of the secret uniform random string R, from the knowledge of the public string P and a reading r' sufficiently close to r. A syndrome-based key-generating scheme called PinSketch is presented in [15]. Similarly to the fuzzy vault, this method is based on polynomial interpolation. Compared with the fuzzy vault, the PinSketch scheme reduces the computational time, and length of the public key. During the enrollment phase, a syndrome based on polynomial interpolation is computed and stored as helper data. During the recognition phase, an error vector is computed from the query biometric sample and the helper data to recover the enrolled biometric. An approach based on multiple biometric traits is presented in [13]. This method is based on the fuzzy commitment scheme. During the enrollment phase, one biometric reading is xored with a random bit string obtained after a pseudo random permutation from the other biometric reading. Differently, during the verification phase, the process is inverted and the second biometric template is reconstructed in order to be used as preliminary check (by comparing the computed hash with the value stored into the identifier) and as input of the matching module. In the literature, there are also other types of key-binding biometric cryptosystem [52, 34].

3.3 Cryptographically secure methods

The recognition accuracy of systems based on cancelable biometrics can be decreased by the applied transformation functions. Similarly, in biometric cryptosystems it is not possible to always adopt the best matching functions used in the plain domain and, as a consequence, the accuracy can be worsened. As a solution to this problem, in the literature there are template protection techniques specifically designed with the aim to perform the biometric recognition without applying transformations of the biometric data and without modifying the matching functions designed for the adopted templates. These methods can directly perform the matching using the encrypted data and are usually based on homomorphic cryptosystems.

In homomorphic cryptosystems, given a set M (resp., C) of the plaintexts (resp., ciphertexts), for any given encryption key k the encryption function E satisfies

$$\forall m_1, m_2 \in M, \qquad E\left(m_1 \odot_M m_2\right) \leftarrow E\left(m_1\right) \odot_C E\left(m_2\right)$$

for some operators $\odot_M$ in M and $\odot_C$ in C, where ← means "can be directly computed from", that is, without any intermediate decryption [20].

The main advantage of these systems is that the accuracy obtained by using the transformed templates is very similar to the accuracy obtained by using the plain data. Usually, a decreasing of the performance can be caused by an excessive quantization or data reduction [5]. The main disadvantage is that it is difficult to adopt homomorphic cryptosystems in biometric systems that require complex matching functions. Homomorphic cryptosystems are also computationally expensive.

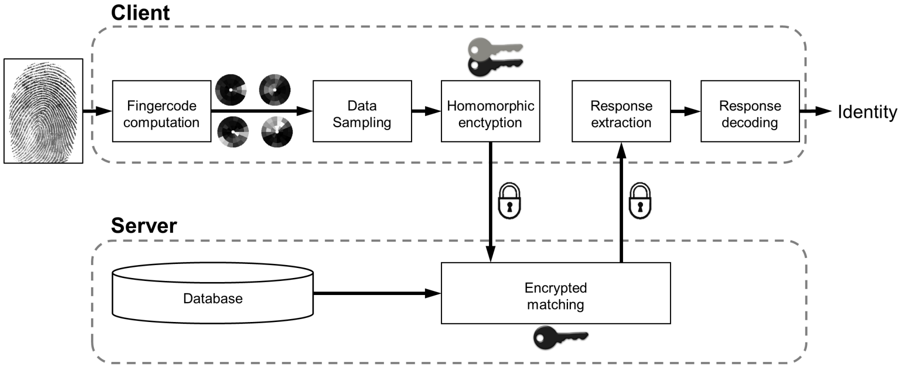

Fig. 6. Example of a cryptographically secure method based on fingerprints. The biometric matching algorithm is processed in the encripted domain exploiting a homomorphic cryptosystem.

A cryptographically secure method designed for distributed architectures is proposed in [4, 3]. This method is based on the fingerprint biometric trait and uses a feature representation called Fingercode [26], which consists in a set of numeric values obtained by applying Gabor filters with different orientations to the fingerprint image. The cryptographic protocol strongly relies on the notion of additively homomorphic encryption and uses two encryption schemes: the Paillier's encryption scheme [41] and a variant of the El Gamal encryption scheme [17] ported on Elliptic Curves. On the client side, the template is computed, quantized and encrypted using the public-key of the client. The server computes the match score in the encrypted domain by exploiting the homomorphic properties of the adopted cryptosystem. The match score consists in the quadratic Euclidean distance between the evaluated templates. During the final task of the recognition process, the server interacts with the client in order to select, in the ciphertext domain, the enrolled identities with the related distances that are below a fixed threshold. Fig. 6 shows the schema of this method.

A similar approach that use the homomorphic encryption is presented in [18, 48] and is designed for face recognition systems. In the literature, there are also approaches based on homomorphic encryption methods and designed for biometric systems that compute the match score as the Hamming distance between feature vectors (e.g. Iriscode [14]): the system in [51] is based on the Blum-Goldwasser cryptosystem, the system in [10] on the Goldwasser-Micali scheme, the system in [8] on the method on homomorphic properties of Goldwasser-Micali and Paillier cryptosystems, the system in [50] on the ElGamal scheme and Garbled Circuits.

4 Conclusions

Relevant privacy and security aspects have to be considered during the design phase and the deployment of biometric systems in order to prevent possible thefts and misuses of biometric data.

The use of biometric data, in fact, presents different privacy risks. Usually, the risks perceived by the users are different from the real risks related to a biometric application. The perceived risks are difficult to evaluate because they are different for each individual. In general, the perceived risks are related to identity thefts and to improperly uses of the personal data (for example, for tracing all the activities of the individuals or for operating proscription lists). Differently, the real risks are related to the applicative context and are determined by different factors, such as the used storage techniques, the owner of the system, the used biometric traits, and other design choices.

In order to properly design a privacy-protective biometric system, it is necessary to follow specific guidelines regarding the treatment of biometric data. These guidelines consider the storage modalities, rights of the users, responsibilities of the operators, and data protection techniques.

In the literature, there are different methods for the protection of biometric data. Most of these methods are designed for the protection of the biometric templates, which are abstract representations of the distinctive features extracted from the biometric samples (signals, images or frame sequences). Template protection methods permit to perform the identity comparison by using protected representations of the biometric templates, and can be divided in three different classes: cancelable biometrics (based on transformations of the templates), biometric cryptosystems (based on cryptographic algorithms that perform the recognition by comparing cryptographic keys), and cryptographically secure methods (based on cryptographic techniques that permits to perform a set of operations without converting the data in the plain domain). The use of these methods can effectively increase the security of the biometric systems, but can reduce the obtained performances in terms of accuracy and computational time. The transformation functions used by cancelable biometrics, in fact, can decrease the accuracy of the recognition system. Similarly, in biometric cryptosystems, it is not possible to always adopt the best matching functions used in the plain domain and, as a consequence, the accuracy can be worsened. Cryptographically secure methods are designed to solve these problems, but are usually based on computationally expansive algorithms and can require a data reduction step in order to increase the speed of the recognition process.

References

1. International Biometrics Group, http://www.ibgweb.com
2. Cancellable biometrics and annotations on biohash. Pattern Recognition 41(6), 2034 – 2044 (2008)
3. Barni, M., Bianchi, T., Catalano, D., Raimondo, M.D., Donida Labati, R., Failla, P., Fiore, D., Lazzeretti, R., Piuri, V., Scotti, F., Piva, A.: A privacy-compliant

fingerprint recognition system based on homomorphic encryption and fingercode templates. In: IEEE Fourth International Conference on Biometrics: Theory, Applications and Systems (BTAS) (September 2010)

4. Barni, M., Bianchi, T., Catalano, D., Raimondo, M.D., Labati, R.D., Failla, P., Fiore, D., Lazzeretti, R., Piuri, V., Scotti, F., Piva, A.: Privacy-preserving fingercode authentication. In: 12th ACM Multimedia and Security Workshop (2010)
5. Bianchi, T., Turchi, S., Piva, A., Donida Labati, R., Piuri, V., Scotti, F.: Implementing fingercode-based identity matching in the encrypted domain. In: IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS). pp. 15 – 21 (September 2010)
6. Boult, T.: Robust distance measures for face-recognition supporting revocable biometric tokens. In: International Conference on Automatic Face and Gesture Recognition. pp. 560 – 566 (April 2006)
7. Boult, T., Schdrer, W., Woodworth, R.: Revocable fingerprint biotokens: Accuracy and security analysis. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR). pp. 1 – 8 (June 2007)
8. Bringer, J., Chabanne, H.: An authentication protocol with encrypted biometric data. In: Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology (AFRICACRYPT). pp. 109 – 124 (2008)
9. Bringer, J., Chabanne, H., Cohen, G., Kindarji, B., Zemor, G.: Theoretical and practical boundaries of binary secure sketches. IEEE Transactions on Information Forensics and Security 3(4), 673 – 683 (December 2008)
10. Bringer, J., Chabanne, H., Izabachène, M., Pointcheval, D., Tang, Q., Zimmer, S.: An application of the goldwasser-micali cryptosystem to biometric authentication. In: Proceedings of the 12th Australasian conference on Information security and privacy (ACISP). pp. 96 – 106 (2007)
11. Cavoukian, A., Stoianov, A.: Biometric encryption. In: Encyclopedia of Cryptography and Security (2nd Ed.), pp. 90 – 98 (2011)
12. Chin, C.S., Jin, A.T.B., Ling, D.N.C.: High security iris verification system based on random secret integration. Computer Vision and Image Understanding 102, 169 –177 (May 2006)
13. Cimato, S., Gamassi, M., Piuri, V., Sassi, R., Cimato, F.S., Scotti, F.: A biometric verification system addressing privacy concerns. In: International Conference on Computational Intelligence and Security. pp. 594 – 598 (December 2007)
14. Daugman, J.: How iris recognition works. In: Proceedings of the International Conference on Image Processing. vol. 1, pp. 33 – 36 (2002)
15. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM Journal on Computing 38(1), 97 – 139 (2008)
16. Draper, S., Khisti, A., Martinian, E., Vetro, A., Yedidia, J.: Using distributed source coding to secure fingerprint biometrics. In: IEEE International Conference on Acoustics, Speech and Signal Processing. vol. 2, pp. 29 –132 (April 2007)
17. El Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Proceedings of CRYPTO 84 on Advances in cryptology. pp. 10 – 18 (1985)
18. Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I., Toft, T.: Privacy-preserving face recognition. In: Proceedings of the 9th International Symposium on Privacy Enhancing Technologies (PETS). pp. 235 – 253 (2009)
19. Faundez-Zanuy, M.: On the vulnerability of biometric security systems. IEEE Aerospace and Electronic Systems Magazine 19(6), 3 – 8 (June 2004)

20. Fontaine, C., Galand, F.: A survey of homomorphic encryption for nonspecialists. EURASIP Journal on Information Security pp. 1 – 15 (2007)
21. Huixian, L., Man, W., Liaojun, P., Weidong, Z.: Key binding based on biometric shielding functions. In: International Conference on Information Assurance and Security. vol. 1, pp. 19 – 22 (August 2009)
22. Ignatenko, T., Willems, F.: Information leakage in fuzzy commitment schemes. IEEE Transactions on Information Forensics and Security 5(2), 337 – 348 (June 2010)
23. Ignatenko, T., Willems, F.: Information leakage in fuzzy commitment schemes. IEEE Transactions on Information Forensics and Security 5(2), 337 – 348 (June 2010)
24. Jain, A.K., Maltoni, D.: Handbook of Fingerprint Recognition. Springer-Verlag New York, Inc., Secaucus, NJ, USA (2003)
25. Jain, A.K., Nandakumar, K., Nagar, A.: Biometric template security. EURASIP Journal on Advances in Signal Processing pp. 1 –17 (2008)
26. Jain, A.K., Prabhakar, S., Hong, L., Pankanti, S.: Filterbank-based fingerprint matching. IEEE Transactions on Image Processing 9, 846 – 859 (2000)
27. Jin, A.T.B., Ling, D.N.C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition 37(11), 2245 – 2255 (2004)
28. Jin, Z., Teoh, A., Ong, T.S., Tee, C.: Generating revocable fingerprint template using minutiae pair representation. In: International Conference on Education Technology and Computer. vol. 5 (June 2010)
29. Juels, A., Sudan, M.: A fuzzy vault scheme. In: IEEE International Symposium on Information Theory. p. 408 (2002)
30. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Sixth ACM Conference on Computer and Communications Security. pp. 28 – 36 (1999)
31. Lee, Y.J., Park, K.R., Lee, S.J., Bae, K., Kim, J.: A new method for generating an invariant iris private key based on the fuzzy vault system. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 38(5), 1302 – 1313 (October 2008)
32. LLC International Biometric Group: Bioprivacy initiative (2003), `http://www.bioprivacy.org/`
33. Maiorana, E., Campisi, P.: Fuzzy commitment for function based signature template protection. IEEE Signal Processing Letters 17(3), 249 – 252 (March 2010)
34. Maiorana, E., Campisi, P.: Fuzzy commitment for function based signature template protection. IEEE Signal Processing Letters 17(3), 249 – 252 (March 2010)
35. Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., Neri, A.: Cancelable templates for sequence-based biometrics with application to on-line signature recognition. IEEE Transaction on Systems, Man and Cybernetic, Part A: Systems and Humans 40(3), 525 – 538 (May 2010)
36. Makrushin, A., Scheidat, T., Vielhauer, C.: Towards robust biohash generation for dynamic handwriting using feature selection. In: International Conference on Digital Signal Processing. pp. 1 – 6 (July 2011)
37. Nagar, A., Jain, A.: On the security of non-invertible fingerprint template transforms. In: First IEEE International Workshop on Information Forensics and Security (WIFS). pp. 81 – 85 (2009)
38. Nandakumar, K., Jain, A., Pankanti, S.: Fingerprint-based fuzzy vault: Implementation and performance. IEEE Transactions on Information Forensics and Security 2(4), 744 – 757 (December 2007)

39. Nanni, L., Lumini, A.: Empirical tests on biohashing. Neurocomputing 69, 2390 – 2395 (2006)
40. Nichols, R.K.: Icsa Guide to Cryptography. McGraw-Hill Professional (1998)
41. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: EUROCRYPT. pp. 223 – 238 (1999)
42. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal 40(3), 614 – 634 (2001)
43. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating cancelable fingerprint templates. IEEE Transaction on Pattern Analysis and Machine Intelligence 29(4), 561 – 572 (2007)
44. Ratha, N.K., Connell, J.H., Bolle, R.M.: An analysis of minutiae matching strength. In: Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA). pp. 223 – 228 (2001)
45. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security (1) (2011)
46. RNCOS (ed.): Electronics Security: Global Biometric Forecast to 2012 (2010)
47. Sabena, F., Dehghantanha, A., Seddon, A.: A review of vulnerabilities in identity management using biometrics. Second International Conference on Future Networks (CFN) pp. 42 – 49 (January 2010)
48. Sadeghi, A., Schneider, T., Wehrenberg, I.: Efficient privacy-preserving face recognition. In: Proceedings of the 12th Annual International Conference on Information Security and Cryptology. LNCS, vol. 5984, pp. 235 – 253. Springer-Verlag (December 2-4, 2009)
49. Savvides, M., Vijaya Kumar, B., Khosla, P.: Cancelable biometric filters for face recognition. In: International Conference on Pattern Recognition. vol. 3, pp. 922 – 925 (August 2004)
50. Schoenmakers, B., Tuyls, P.: Computationally Secure Authentication with Noisy Data, pp. 141 – 149. Springer-Verlag, Berlin, Heidelberg (2007)
51. Stoianov, A.: Cryptographically secure biometrics. In: Kumar, B.V.K.V., Prabhakar, S., Ross, A.A. (eds.) Biometric Technology for Human Identification VII. vol. 7667, p. 76670C. SPIE (2010)
52. Sutcu, Y., Li, Q., Memon, N.: Protecting biometric templates with sketch: Theory and practice. IEEE Transactions on Information Forensics and Security 2(3), 503 – 512 (September 2007)
53. Teoh, A., Goh, A., Ngo, D.: Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence 28(12), 1892 – 1901 (December 2006)
54. Teoh, A., Jin, B., Connie, T., Ngo, D., Ling, C.: Remarks on biohash and its mathematical foundation. Information Processing Letters 100, 145 – 150 (November 2006)
55. Wang, Y., Hatzinakos, D.: On random transformations for changeable face verification. IEEE Transaction on Systems, Man and Cybernetic, Part B: Cybernetics 41(3), 840 – 854 (June 2011)
56. Wang, Y., Plataniotis, K.N.: An analysis of random projection for changeable and privacy-preserving biometric verification. IEEE Transaction on Systems, Man and Cybernetic, Part B: Cybernetics 40, 1280 – 1293 (October 2010)