1 Privacy in Biometrics

Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Roberto Sassi and Fabio Scotti

University of Milan, Department of Information Technologies, via Bramante 65, 26013 Crema (CR), Italy

Biometric features are increasingly used for authentication and identification purposes in a broad variety of institutional and commercial systems, such as e-government, e-banking and e-commerce applications. On the other side, the adoption of biometric techniques is restrained by a rising concern regarding the protection of the biometrics templates. In fact, people are not generally keen to give out biometric traits with little assurance that they cannot be stolen or used without an expressed consent. Recent results showed that generating a unique identifier by combining biometric traits making it impossible to recover the original biometric features (thus preserving the privacy of the biometric traits) is feasible. The chapter reviews the privacy issues related to the use of biometrics and presents some of the most advanced techniques available up to date, providing a comparative analysis. and giving an overview on future trends.

—

1.1 INTRODUCTION

Biometric features are increasingly used for authentication and identification purposes in a broad variety of institutional and commercial systems. The large diffusion of e-government, e-banking and e-commerce applications requires more stringent methodologies to identify customers or citizens in order to prevent any malicious behavior which could lead to economic loss or fraud attempts for the involved parties. Biometric data are natural candidates to be used in authentication systems which should guarantee an higher level of security. Such kind of data are indeed unique for each person and strictly associated to its owner. They are irrevocable, in the sense that the association cannot be changed during the human life and in many cases they are hard to forge.

Many different authentication systems have been proposed taking into account different biometric traits, some physiological, some behavioral, each proposal having different advantages or drawbacks. In some cases, practical settings have been

devised and different solutions are available in commercial applications or for border control. If from one side the interest in biometrics techniques is more and more increasing for their advantages (security, reliability, etc..) on the other side, the potential threats to the privacy of users, coming from the abuse of biometric information, is object of discussion and often prevent the adoption of biometric systems on a large scale. In fact, people are not generally keen to give out biometric traits with little assurance that they cannot be stolen or used without an expressed consent. For the same reason discussed above, many people are more and more worried about the adoption of biometric systems in practical situation.

Recently, much research work has been devoted to the construction of techniques for the protection of biometric templates. In this way, biometric authentication schemes can be devised, satisfying the increasing request for privacy coming from users. Such techniques usually enable the generation of secure identifiers after a transformation of the input biometric traits making it impossible to recover the original biometric features (thus preserving the privacy of the biometric traits). Several proposals have been formulated combining cryptography and biometrics in order to increase the confidence in the system when biometric templates are stored for verification.

The chapter reviews the privacy issues related to the use of biometrics and presents some of the most advanced techniques available up to date, providing a comparative analysis and giving an overview on future trends. The chapter is structured as follows. In the next section we present the most common biometric traits and features used in real-world applications as well as the associated risk level in the privacy for the individuals. In Section 1.3 we introduce efficient representation of biometric features in order to protect biometric templates and construct privacy compliant authentication system. In Section 1.4 we discuss privacy issues in multimodal biometric systems, when more than one biometric trait is used, and present in Section 1.5 an innovative method for building multimodal privacy-aware verification system.

1.2 BIOMETRIC TRAITS AND PRIVACY

In this section we discuss the privacy issues concerning the practical usage of the biometric systems. To this purpose it is important to consider both the view of users and the real risks which they could be exposed to. Different perspectives about privacy can also be given w.r. to the application context in which biometrics are exploited and the particular methodology used for the collection of biometric data. Finally privacy risks can also be evaluated considering the specific traits which the biometric systems are based on.

1.2.1 User perception and real risks

The users commonly perceive biometric authentication and identification techniques as a threat to their privacy rights. In particular there are some aspects that enforce this perception [18]. The first one is related to the fact that the acquisition of the

biometric traits is considered as an exact and permanent filing of the user's activities and behaviors. For example, it is very common the thought that most biometric system has 100% identification accuracy and that the biometric samples and templates are necessarily stored and/or sent over a network, exposing them to further risks of being exposed. Actually, the latter is a well founded concern. In fact, while it should be granted to the user that the biometric information collected should not be used for any other activities than the ones expressly declared, in some cases it is harder to grant this aspect, especially if the biometric samples themselves are sent over a network. The second issue is related to the possibility to track down the user activities associated to the biometric acquisition, even in the far future. This leads to produce in the users the perception of the possibility to be "tracked" in his movements, or his buying and life style. Commonly this issue is associated to a sort of "big brother" phobia, in which a superior entity is capable of observing and acquiring knowledge on each activity of the user.

In a negligible part of the population, the usage of a biometric system is also perceived as uncomfortable or dangerous. For example, the fingerprint sensor – when previously used by other people and not properly cleaned – can be considered as unpleasant or disgusting. Or face and iris acquisition systems might induce apprehension to have the eyes damaged by lasers and/or IR sources. Very interestingly, users often overlook others privacy related problems arising when biometrics are involved.

The first point concerns the possible usage of biometric information for operating *Proscription Lists*. For example, a user can be classified from a previous behavior or activity in a specific class, and then – as a consequence of this classification – some services and accesses can be denied. Important examples of this situation are the black lists present in call centers and service providers especially designed to identify and to manage the users considered as "offending" or "not-collaborative". Other examples are the "bad-credit" lists filled in many investor and mutual founds companies. Indeed, proscription lists can be employed also without the adoption of biometric systems (and actually they are), but the usage of biometric technologies can make the situation more and more dramatic.

The second point concerns the fact that many biometric features can be used to *obtain personal information* of the users, such as medical information of past illnesses or the current (and future) clinical trends. For example, the retinal pattern acquired by the biometric system can produce valuable information of the presence of hypertension, diabetes and others illnesses [17]. Much more personal information can be extracted from DNA samples [15].

1.2.2 Applicative contexts

The real risk of privacy invasiveness can be analyzed in more detail with respect to both the final application which the biometric system is dedicated to and the biometric trait which is involved. Table 1.1 plots a qualitative representation of the privacy risks versus ten different application features, according to the International Biometric Group [16].

Table 1.1 Applicative aspects concerning the privacy (according to the IBG)

Lower ← Risk of privacy invasiveness → Greater		
Overt	↔	Covert
Optional	↔	Mandatory
Verification	↔	Identification
Fixed Period	↔	Indefinite
Private Sector	↔	Public Sector
Individual, Customer	↔	Employee,Citizen
Enrollee	↔	Institution
Personal Storage	↔	Database Storage
Behavioral	↔	Physiological
Templates	↔	Images

Biometric *covert applications* (such as the surveillance systems without explicit authorization from the users) are considered to be more privacy invasive. On the other hand, the biometric systems for identification or verification that are *optional* are considered as more privacy compliant. In this case, users can decide to not be checked by a biometric system, and they can adopt a different identification/verification system.

Privacy is considered to be exposed to a greater risk when the biometric system performs an *identification* instead of a simpler verification task. That is related to the fact that the identification process encompasses a "1-to-many" comparison, which, in most cases, is not carried out in the same place of the acquisition (typically, the biometric data is sent trough a network to a database for the comparisons).

Also the *duration* of the retention of the biometric data impacts the privacy risk. If retention expires in a fixed period of time, the privacy risk is reduced. Best practice notions require that every project which encompasses biometric data retention should always explicitly state its duration.

Different risks are present with respect to the sector of application: the biometric setups in the *public sector* are considered to be more susceptible to privacy invasiveness than the same installations in the *private sector*.

Also the *role* of the individuals that use the biometric system has great impact on the privacy. There roles have an increasing privacy risk: individual, customer, employee, citizen. The most relevant privacy invasion is related to the association of the fundamental rights of the individual to a biometric identity test. The privacy risks are lower in the applications where the individuals retain usage rights over the biometric data.

Also the *storage method* of the biometric data affects the privacy risk. The worst case is when they are all stored in a central database, out of the user's control. The best case is when the user personally holds the biometric data, for example when the personal biometric information is stored only on a smart card belonging to the users.

The distinction between behavioral and physiological traits is relevant with respect to the privacy risks. The *physiological data* (such as fingerprints, or iris templates)

Table 1.2 Data Collection Approaches

Approach	Examples
Protective	Enterprise Security, Accountholder verification
Sympathetic	Application of the Best practice notions in common applications
Neutral	Personal PCA, Home PC, Access control
Invasive	Surveillance, some Centralized National ID Services

can be used in a more invasive manner. That is related to the fact that the physiological traits are the most stable in time and they are characterized by very high verification/identification accuracies. On the other side, the *behavioral traits* tend to be less accurate, and, most of the time, they request the user collaboration.

Also the storage format is relevant: *templates* are usually carrying much less information than the original sample/images. While they are less powerful when used as direct identifiable data, they are privacy-invasive.

1.2.3 System design and data collection

Another useful taxonomy concerns the different approaches for biometric data collection and storing. The IBG classifies four different classes concerning the privacy protection (Table 1.2): Protective, Invasive, Neutral, Sympathetic [16].

A *privacy-protective* system is designed to protect or limit the access to personal information, providing a means for an individual to establish a trusted identity. In this case, the biometric systems use biometrics data to protect personal information which might otherwise be copied, stolen or misused.

A *privacy-sympathetic* system limits access/usage to personal data. A privacy-sympathetic approach encompasses the specific design of elements able to protect biometric data from unauthorized access and usage. Also the storage and the transmission of biometric data must be informed, if not driven, by privacy concerns.

In a *privacy-neutral* system, privacy aspects are not important or the potential privacy impact is slight. Privacy-neutral systems are designed to be difficultly misused with regards to privacy issues, but they do not have the capability to protect personal privacy.

A *privacy-invasive* system facilitates or enables the usage of personal data in a fashion which is contrary to privacy principles. In privacy-invasive systems personal data are used for purposes broader than what originally intended. Systems which facilitate the linkage of personal data without an individual's consent, and those in which personal data are loosely protected belong to this class.

1.2.4 Technology evaluation

The different biometric technologies associated to each biometric trait can produce various levels of privacy risk. In Table 1.3 it has been plotted the overall risk for

Table 1.3 Privacy risk ranking with respect the available technologies (Verif. = verification; Id. = identification; Behav. = behavioral; Phys. = physiological; Ov. = Overt; Cov. = Covert; DB Comp. = Database compatibility).

Trait	Verif./Id.	Behav./Phys.	Ov./Cov.	DB Comp.	Overall risk
Face	high	medium	high	high	high
Fingerprint	high	high	low	high	high
Retina	high	high	low	low	medium
Iris	high	high	low	low	medium
Hand	low	medium	low	low	low
Voice	low	low	medium	low	low
Keystroke	low	low	medium	low	low
Signature	low	low	low	low	low

the user's privacy associated to the specific trait. The privacy related aspects are summarized by taking into account the four most significant technologies features [16].

The first feature is associated to the capability of the technology to process searches in databases of biometric records. The higher this capability, the higher the privacy risk.

The second feature is associated to the possibility of the technology to effectively work in an overt or covert fashion. For example, a face recognition system can be more likely used in a covert manner than a classical fingerprint system. The higher this capability, the higher the privacy risk.

The third feature tends to distinguish the behavioral traits from the physiological ones. The acquisition of most behavioral traits need cooperation from the user and they are less stable in time, hence they are considered to be more privacy compliant than the physiological. The higher the need of user cooperation or the variability in time, the lower the privacy risk.

The forth feature is related to two points: the technology interoperability when working with different databases, and the presence of numerous and/or large available databases to process comparisons. For example, a face acquisition can be used for multiple search in different databases with relatively low efforts. Similarly, many – and large – databases of fingerprints templates exist and they can be queried using fingerprints taken with different sensor and techniques. Summarizing: the higher the interoperability and the presence of available databases, the higher the privacy risk.

The last column of the Table 1.3 reports the overall risk of the relative technologies obtained by qualitatively weighting all the feature scores.

1.2.5 Best practice for privacy assessment in biometrics

It is worth noting that the biometric features, samples and templates can not be considered as "secrets" since it is possible to capture them to create real or digital

artifacts suitable to attack a biometric system [18]. But, in any case, the protection of the biometric data is absolutely essential from many points of view such as privacy and security issues [29].

The design and the usage of a biometric system should always respect strict guidelines in order to protect the user privacy. These notions encompass four main points [16]: i) the scope and the capabilities of the system; ii) the data protection; iii) the user control of personal data; iv) the disclosure, auditing and accountability of the biometric system. In the following discussion, we refer to two main classes of actors: the users and the operators who manage the biometric system.

The first point concerns the *scope and the capabilities of the system*. First of all, the scope and the functionalities of the system should not be expanded without the explicit and informed consensus of all the users. From the capability point of view, the retention of the biometric information must be limited to the minimal amount. In general, the biometric system stores the enrollment data, but the verification data should always be deleted. Only templates should be recorded: any row data, images and recordings should be deleted as soon as possible during the functioning. Also the collection of other information should not happen and absolutely should not not be integrated into the biometric data. In addition, the termination date of all system functionalities should be provided, or, at least, the deletion date must be communicated to the user.

The second point focus on *data protection*. The use of proper techniques to protect the biometric data should always be considered. Suitable examples are the adoption of encryption primitives and private networks which must be designed and managed using the state-of-the-art best practices. Systems should also be hosted in secure and controlled areas. These condition must be ensured for all the life cycle of the biometric system. It is important to note that also the result of the matching phase (the "match", "non-match", and errors cases) must be protected and considered as private information. The final issue concerns the limitation of the access of the biometric data to a well-defined and limited group of operators.

The third point is related to the *user control of personal data*. The guidelines foreseen that the user must keep the control on her/his biometric data. The biometric system should be used voluntarily by the user, and, in any case, the system must ensure to the user the possibility to be un-enrolled. In addition, the user should be always able to correct and modify her/his personal data.

The forth point describes the *disclosure, auditing and accountability* of the biometric data. The exact purpose of the biometric system must be explicated to the operators and the enrollees. In particular, it must be explained if the biometric acquisition is optional or compulsory. It is important to disclose when the biometric system is used, especially when enrollment and verification or identification phases are carried on. The guidelines suggest also that each operators must be accountable for the possible missuses/errors perpetrated during the working activities. Also suitable procedure must be considered in order to solve disputes concerning the usage of the biometric system. The owner of the biometric system and the operators must also be able to provide a clear and effective process of auditing when an institution

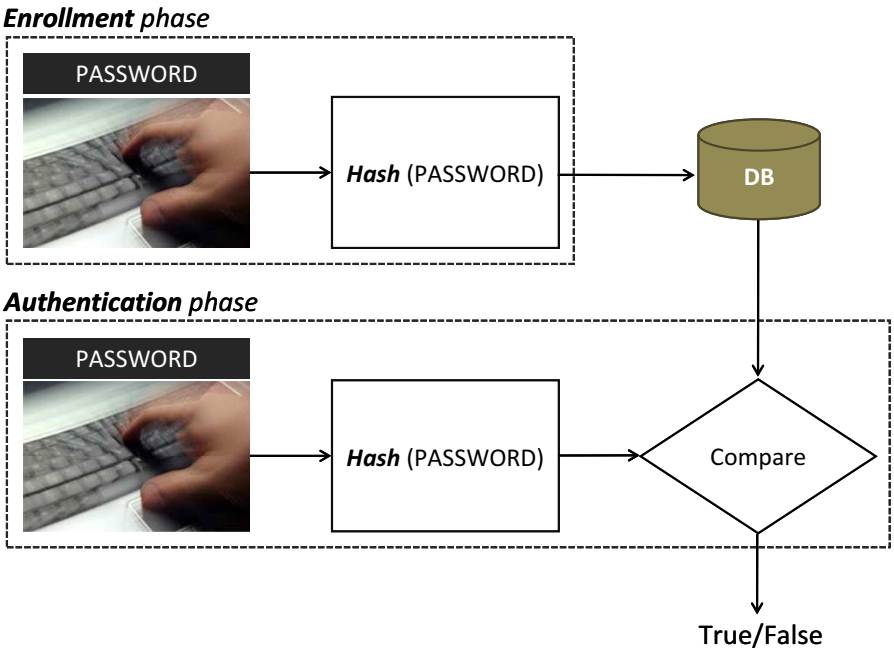

Fig. 1.1 Password based authentication scheme.

or a third party must perform a critical review of all the modules which compose the biometric system.

A broad and rapidly growing literature is focused on the goal of protecting and augmenting the privacy protection of a biometric system. In the following part of this chapter we will focus in particular on the multidisciplinary approaches which encompass biometric and cryptographic techniques.

1.3 BIOMETRIC TEMPLATES PROTECTION

Much work in the literature has been devoted to the construction of techniques for the protection of biometric templates in biometric based authentication schemes. The naive approach of storing biometric templates during the enrollment phase (for the successive identification of verification process) in a more or less secured database has a number of risks for users privacy. The strict association between each user and his biometric templates raises concerns on possible uses and abuses of such kind of sensible information, since biometrics traits cannot be replaced or modified. A stolen template after an unauthorized access to the database could help a malicious user to impersonate a legitimate user and steal private information or run applications accessing sensible resources. The loss of biometric data is then an important security

issue which directly affects the valuation of a biometric authentication schema and should be carefully considered to prevent thefts of identity [29].

In many communities (in Europe see the Biometric Identification Technology Ethic (BITE Project) [5]), groups of researchers are investigating the legal background of biometric technologies, to define and consider bioethical issues arising from emerging biometric identification technologies. Different countries are adopting strict rules to limit the impact of biometric technologies on the privacy of citizens. The proposed authentication schemes often have to face the legal constraints imposed by such directives considering the risk of function creep and data misuse.

To protect users privacy, biometric templates are usually transformed before their storage during the enrollment phase, such that the authentication process can be correctly performed, but unauthorized access to the stored templates leaves the adversary with a small and unusable amount of sensible data on the biometrics of the attacked user. A natural way to protect biometric templates could be to replicate the approach used in password based authentication schemes where users' passwords are typically stored in their hashed form (see Figure 1.1). Due to the mono-directionality of the used hash functions, the knowledge of the hashes does not gives any information; so if the database has been corrupted the passwords are not compromised. For biometric templates, things are more complicated since usable one way transformation of the templates are not so easy to achieve. Indeed the higher variability within different readings of biometric data makes them unsuitable to be directly used as input for hash functions or as cryptographic keys.

In the literature, a wide range of techniques have been presented based on the combination of biometrics and cryptography, in order to cope with both problems: variability of biometric templates and protection of personal data. A comprehensive survey of different approaches and of the related problems can be found in [35]. The process of generating cryptographic keys from biometrics generally relies on an error tolerant representation of the biometric features or on the selection of a distance preserving robust transformation operating on the biometric template. The transformation of biometric templates in a suitable representation which can be efficiently treated, for example in a metric space, is itself an active research area [34]. IrisCode [9] and Fingercode [19] are techniques for the extraction of a binary string from iris and fingerprint templates, respectively. The referred model is depicted in Figure 1.2, where a string representation is extracted from the considered biometric feature and successively a non invertible transformation is applied in order to securely store the biometric template. The same transformation is applied to the fresh biometric templates acquired during the authentication phase, and the biometric match succeeds if the two obtained transformations are equal or sufficiently close. The non invertibility of the transformation ensures that an adversary does not get any valuable information even if he gets or steals the stored (transformed) template.

Another recently developed approach relies on the extraction of *helper data* during the enrollment phase which is stored together with the hashed form of the biometrics. Such data can be made publicly available and is used in the authentication phase in combination with fresh biometric features in order to reconstruct the derived secret. The recently introduced fuzzy cryptographic primitives [12], *secure or fuzzy*

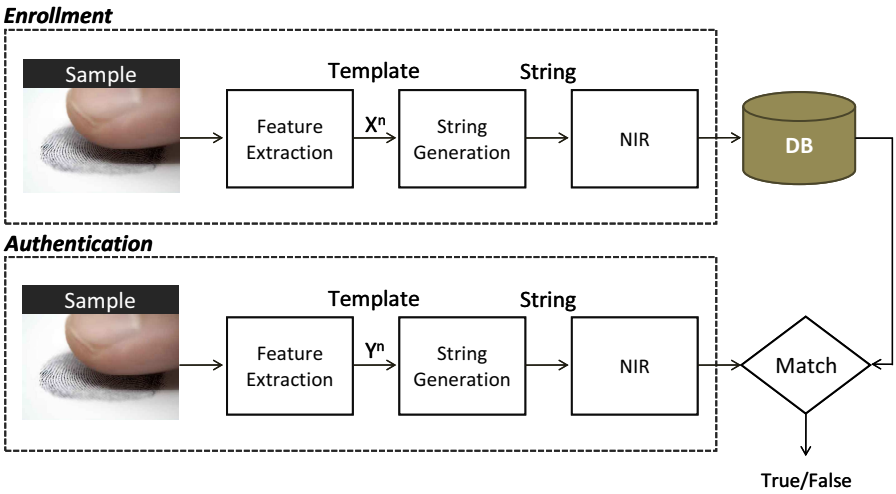

Fig. 1.2 A biometric authentication scheme with a non invertible transformation (NIR).

sketch and *fuzzy extractor* build on this principle and allow the secure extraction of a uniformly random string from the (biometric) input in a noise-tolerant way. Based on this primitives, recently several constructions for devising practically usable biometric authentication systems have been proposed [32, 33].

1.3.1 Hash based transformations

Hash based biometric authentication schemes, rely on variations of hash functions, ensuring a robustness property so that small changes in the input biometric samples produce the same hash value. In Davida *et al.* [10, 11], "robust" hash functions are used to protect the sensitive user template avoiding the need of storing the biometric template in the database. Different kinds of comparison between the hashed templates are used in the one-way transformation combined with a secure cryptographic hash function. The one-way transformation is designed as a combination of various Gaussian functions to behave as a robust hash scheme. Then, the hash function is used to cryptographically secure the biometric templates stored in the database.

Such techniques have been applied taking into account different biometric traits. In [37] a similar technique has been defined for signatures. In this application a pen-based PDA is used to collect a signature which is transformed into a hash value. Then, the hash value is also used to create a key for a secure data communication channel. The authentication is not made using a typical biometric signature comparison but using a vector of hash values, composed by 24 features extracted from the signature. The method uses a statistical approach: during enrollment, 4 signatures per user are required to build a personal interval matrix which will be stored in the database. The final decision is made by comparing the fresh hash values in the vector with the stored interval matrix of each individual present in the database. In [8] palmprint biometrics

has been considered. The features of palmprints are extracted from the palm images, then the Fisher Discriminant Analysis is applied to select the most significant ones producing a reduction of the space dimensionality. This set of features is then combined with a randomized number (the token) by the "PalmHashing" algorithm achieving a discretization process. This algorithm projects the biometric input into a orthonormal base produced by the randomized number (the token) using the well-known Gram-Schmitd process.

The *Biohashing* technique has been introduced in [20] and relies on the usage of a two-factor authenticator combination of pseudo-random numbers and a biometric binarized feature. The main disadvantage of the BioHashing method is that poor verification performances are displayed when an impostor steals the pseudo-random number used to build the ID of a genuine and tries to authenticates as the genuine [25]. The usage of a multi-modal biometric authentication system where one or two biometric features have been "biohashed" is shown to reduce the effect of this drawback, but the proposed technique increases the overall Equal Error rate. In [21] a biohashing approach is used to produce the Facehashing algorithm. In this case, the face images are pre-processed using the Fourier-Mellin wavelet transformation in order to obtain a low-frequencies face representation. The resulting representation is more robust with respect to facial expressions and small occlusions. Then, a discretization process is defined, achieved by a repeated inner-product of the used data and an orthonormal base obtained with a secret number (the token) using the Gram-Schmitd process. The final hashed data are considered to be a zero-knowledge representation of the user input. In [24] the face is used to produce a non-reversible binary template by using a recognition of fiducial points (eyes, nose, eyebrows) and the application of a set of Gabor filters to the face images. The quantization of the extracted features is then processed using a comparison between the obtained features vector from the face and the mean features vectors present in the database. Every bit in the binary template is associated with a reliability estimate based on the standard deviation of its corresponding feature. The most reliable components of the vector after quantization are used to compose the final binary template. The matching function has been designed using a correlation quantifier.

A different approach aims at building a transformation operated on the original biometric template, that is difficult to be inverted, but which can preserve similarity. In [28] a general scheme is proposed to produce a non-invertible function capable to transform a point pattern (for example the minutiae set present in a fingerprint or the frequency-amplitude parameters of a speech pattern) using high-order polynomials. In [1] it has been proposed a transformation and matching algorithm for fingerprints. The transformation is based on geometric translations of the minutiae coordinates and their angles. Such transformation depends on a key and is considered not-reversible. Changing the key, it is possible to produce a new transformed template from the same fingerprint. Unfortunately, the study does not provide a complete analysis of the security of the scheme, focusing only on the error rates. A deeper insight on geometrical and functional transformations in fingerprint biometrics is given in [27]. The study compares the capability of the cartesian, radial and functional transformations in producing cancelable biometrics. This approach provide flexibility to

change the transformation from one application to another to ensure the security and privacy of biometric data. The paper demonstrates the non-reversibility by proving that it is computationally hard to recover the original biometric identifier from a transformed version. A similar approach has been proposed in [30] to achieve a biometric system for offline verification of certified, cryptographically secure documents. The presented technique can produce printable IDs obtained from an extracted and compressed iris feature and an arbitrary text.

In most of the presented approaches rigorous security analysis is missing. In particular, it is not clear the real robustness of these schemes once the hash values/function are also compromised (or the transformed-templates/transformation-algorithm for the second approach), as well as the related keys and parameters (*i.e.*, the tokens)

1.3.2 Cryptographic Fuzzy Primitives

A different set of techniques coping with the variability of biometric templates, is based on the use of error correction codes aiming to extract an unique associated feature from each different biometric reading: the different readings are treated as corrupted codewords and are accordingly decoded. During the verification phase, the feature retrieved by a biometric reading is given as input to an hash function, and compared with the hash value stored during the enrollment phase.

A generalization of this basic approach has been proposed by a group of researchers which introduced fuzzy cryptographic primitives, *i.e.* fuzzy or secure sketch and fuzzy extractor, which can be used in different field of applications and biometric authentication scheme as well. Such constructions usually do not rely on a particular metric space even if most of the constructions have been given considering Hamming distance. However set difference and edit distance metrics have also been considered, referring to the size of the symmetric difference of two input sets in the first case and to the number of insertions and deletions needed to convert one string into the other, in the second case.

1.3.2.1 Fuzzy Commitment In [23], Juels and Wattenberg proposed the "fuzzy commitment" scheme where a secret message is protected using a biometric template. In this case, an error correcting code is used in order to associate a codeword c with a person and to compute an offset ($\delta = c \oplus x$) for the biometric template x. The encrypted message (the *fuzzy commitment*) is then represented by the pair $(\delta, h(c))$, where $h(c)$ is a one way hash function. It is worth to notice that neither the biometric feature, nor the associated codeword are publicly stored. The authentication process is correctly performed if a fresh biometric reading y allows the computation of a binary string $c' = \delta \oplus y$ sufficiently close to c so that the code decodes it to c and the comparison between their hash values succeeds.

A similar construction has been proposed by Hao *et al.*, with the application of an iris code feature extraction algorithm and the combined use of Hadamard and Reed-Solomon codes [14].

1.3.2.2 Fuzzy Vault Juels and Sudan proposed a "fuzzy vault scheme" in [22] relying on the polynomial interpolation technique in order to cope with variability of the stored biometric template. With such technique the problem of having an order invariant representation of the biometric template is overcome. The basic idea is to lock a secret in a vault using an unordered set. The secret could be successfully retrieved using another unordered set which substantially overlaps with the first used set. More in detail, the secret is encoded using the evaluation of a polynomial over a given set of points using the Reed Solomon encoding scheme, *i.e.*, such points represent a codeword. To increase the security, a set of *chaff* points are added to the first set in order to form the vault. To reconstruct the codeword, the user has to provide a set of points which overlaps with the original set.

The fuzzy vault construction has been successfully applied by Uludag and Jain using fingerprint templates [36]. Clancy *et al.* proposed a construction of a biometric identification schema using a secure smartcard to store the vault [7]. Their construction however has been slightly modified in order to cope with real life parameters. Finally the problem of the selection of chaff points, avoiding that the attacker get enabled to distinguish between chaff and real points has been considered by Chang and Li [6]. Some bounds on the entropy loss have also been introduced.

1.3.2.3 Fuzzy Sketch and Fuzzy Extractor An important step towards the realization of personal identification system based on cryptographic key derived from biometrics features has been recently done by Dodis *et al.* [12]. In their work, novel primitives were introduced, the *secure or fuzzy sketch* and *fuzzy extractor* which find a natural application in such kind of systems.

Fuzzy sketches resolve the problem of error tolerance, enabling the computation of a public string P from a biometric reading r, such that from another reading r' sufficiently close to r it is possible to reconstruct the original reading. Furthermore the knowledge of P, should not reveal too much information on the original reading r, *i.e.* the entropy on r is enough to be useful even if P is public. 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 fuzzy sketches. Indeed, fuzzy extractors can be built out of fuzzy sketches and enable the recovering of the secret uniform random string R, from the knowledge of the public string P and a reading r'sufficiently close to r.

To present more formally the fuzzy primitives and the associated constructions, we introduce the basic notions. In particular, even if different metric spaces have been considered in [2], we focus only on Hamming distance metric, and the fuzzy commitment construction of Juels *et al.*, which can be easily turned in a more robust fuzzy extractor primitive.

A metric space $\mathcal{M}$ is a finite set equipped with a non negative distance function $d : \mathcal{M}x\mathcal{M} \rightarrow \mathcal{R}^+$. Consider the Hamming space $\mathcal{H}$, where $\mathcal{M} = \Sigma^n$ for some alphabet Σ and the Hamming distance which for two strings $w, w' \in \Sigma^n$ returns the number of bits in which the two words differ. A $(\mathcal{M}, m, m', t)$-fuzzy sketch is a pair (Fsk, Cor), where:

- Fsk is a (typically) randomized sketching function that on input $w \in H$ outputs a sketch $P \in \{0,1\}^*$, such that for all random variable W over H with min-entropy $H_\infty(W) \geq m$, the average min-entropy of W given Fsk(W) is a least m'.

- Cor is a correction function which enables the recover of w from its sketch and another vector w' close to w: given a word $w' \in H$ and a sketch P, outputs a word $w'' \in H$ such that for any $P = Fsk(w)$ and $d(w, w') \leq t$, it holds that $w'' = w$.

A $(\mathcal{M}, m, l, t, \epsilon)$-fuzzy extractor is a pair of procedures generate *Gen* and *Rep*, where:

- *Gen* is a randomized generation function that on input $w \in \mathcal{M}$ extracts a private string $R \in \{0,1\}^l$ and public string P such that for all random variable W over $\mathcal{M}$ with min-entropy $H_\infty(W) \geq m$, it holds that r is close to uniform even for who observers P, i,e, the statistical distance $D(R, P)(U_l, P) \leq \epsilon$.

- *Rep* is a regeneration function which given a word $w' \in H$ and a public string P, outputs a string S, such that if $d(w, w') \leq t$, and $(R, P) = Gen(w)$, it holds that $Rep(w', P) = R = S$.

The first property (security) guarantees the uniformity of the extracted secret string R (remember that the min-entropy , the second property (correctness) guarantees the correctness of the reproduction.

In this setting it is possible to show that the fuzzy commitment construction of Juels and Wattenberg is a a $(\mathcal{M} = \Sigma^n, n, k, t, 0)$-fuzzy extractor when a a binary linear code C of length n, dimension k and correction capacity t, i,e, with parameters $[n, k, 2t + 1]$, is used, and when W is uniform (*i.e.*, $m = n$). In this case $Gen(w)$, where $s = w - C(x)$, returns $R = x$ and $P = s$. To execute, $Rep(w', P)$, decode $w' - P$ to obtain $C(x)$ and apply the decoding function to obtain x. Notice that s is random when also w is random, and if W is not uniform, s would leak information about x. In general it is possible to obtain for a given code C with parameters $[n, k, 2t + 1]$ and any m and ϵ a (M, m, l, t, ϵ) fuzzy extractor with $\ell = m + k - n - 2 * log(1/\epsilon) + 2$, by using in the extraction phase pairwise independent hashing.

In a successive work [2], Boyen pointed out how multiple use of the same fuzzy secret can cause some security problem, introducing outsider and insider attack scenarios, where an adversary tries to obtain information on the secret by performing repeatedly extractions and regenerations of the fuzzy secret. In such scenarios, with some limitations, it is possible to show that information theoretic security can be achieved and existing constructions can be adapted to satisfy the additional requirements. More general attack models and constructions to achieve secure remote biometric authentication are proposed in [3]

1.3.2.4 Fuzzy based authentication schemes Since the introduction of the fuzzy primitives, many researchers have proposed several authentication schemes based on

the applications of such techniques. A general framework to design and analyze a secure sketch for biometric templates is presented in [32], where the face biometrics have been used as example. Interestingly, the paper shows that theoretical bounds have their limitations in practical schemes. In particular, it has been shown that the entropy loss of the template can not be considered a complete description of the robustness level of the scheme in practical application, while the analysis of the FAR and FRR should be always envisioned. In [4] a near-optimal error-correcting code is discussed (based on a two-dimensional iterative min-sum decoding algorithm) for application with iris biometrics in a fuzzy sketches scheme. The paper produces also an explicit estimation of the upper bounds on the correction capacity of Fuzzy Sketches on iris-based biometrics. A fuzzy based construction for fingerprint biometrics has been discussed in [33], where the string representation of the biometric templates relays on Fingercodes.

1.4 PRIVACY IN MULTIMODAL SYSTEMS

Humans beings typically identify other individuals using a biometric approach which encompasses more than a single biometric trait. For example we can recognize a person watching his face, but the final decision is often integrated using other biometric traits such as the voice, the stature, the gait, or the behavior. In a similar way, a multimodal biometric system uses different biometric traits and combines them efficiently [31]. More in detail, in the literature the term *multibiometric system* is used when different approaches are considerd. In particular, the term is used when one or more of the following setups are present: -multiple sensors (*e.g.*, solid state and optical fingerprint sensors), -multiple acquisitions (*e.g.*, different frames/poses of the face), -multiple traits (e.g, an eye and a fingerprint), -multi instances of the same trait kind (*e.g.*, left eye, and right eye), -multiple algorithm (e.g, different preprocessing and/or matching techniques). In this framework, a multimodal system is a case of a multibiometric system.

The usage of multimodal systems has an heavier impact on the privacy of the user since the amount of the involved personal information is greater. This issue can be better understood taking into account the specific peculiarities of multimodal systems.

1.4.1 Pros and cons of multimodal systems

The multimodal approach has several positive aspects. For example, typically, the performance of a matching system is improved with respect to the same system working with the single traits which compose the multimodal system. Using different traits, it is possible for these systems to increase the population coverage, since some individuals can not have one or more biometric traits (illnesses, injuries, etc.). In addition, the global fault tolerance of the system is enhanced, since, if one biometric subsystem is not working properly (*e.g.*, a sensor problem occurred), the multimodal

system can keep working using the remaining biometric submodules that are correctly functioning.

The multiple acquisition of different traits at the same time (or in a very narrow time frame) achieves an effective deterring against spoofing actions. Also the efficiencies of the database management can be improved by indexing techniques.

In particular, the performances of a multimodal system are improved when uncorrelated traits are used (for instance an eye and a fingerprint, the right eye and the left eye).

The usage of multimodal biometric systems has also some important drawbacks. The first is related to the higher cost of the systems, since they are composed by multiple and different biometric subsystems, each for every single traits that has been selected.

A second aspect is related to the acquisition time: a multi-acquisition is mostly longer than a single acquisition. In addition, the user can perceive the multiple acquisition as more invasive and/or inconvenient.

A third point is associated to the fact that the retention of biometric data is proportionally larger in the case of multimodal biometric systems. Hence, the privacy issues discussed in previous sections of this chapter became much more relevant [26].

1.4.2 Design of privacy compliant multimodal systems

Proper guidelines for the design of the multimodal systems can reduce the described drawbacks and encourage its use in a wide range of application for authentication. Hence, in addition to the guidelines described in previous sections, the following key points should be considered:

- The usage of the templates should be subjected to randomization transformation such that the derived published identifier do not suffer from information leakage.
- When designing a multimodal system it should be carefully taken into account the *number* of samples and the *types* of the biometric traits. For example, less biometric traits should be acquired for a low-security application (*e.g.*, the access to a transport system) than a high-security application (*e.g.*, the access to a nuclear plant). Accordingly, also the choice of the kinds of traits to be used by the multimodal system is relevant with respect to the privacy of the user as discussed in the previous sections.
- Multiple biometrics readings should be combined in order to adapt the security of the authentication system to the level requested by the running application. For example, if the same multimodal biometric system is adopted on the same building/area (such as an airport terminal), each restricted area with different levels of security should be accessed by using different traits or combination of traits.
- The multimodal system should be modular in order to not rely on a proprietary algorithm. In this case, the discovery of novel techniques for biometric

recognition can be easily embedded in the system, in particular, taking into the account new techniques and new template formats which are more privacy compliant.

- Proper protection techniques must be envisioned in order to avoid that each biometric sample/template/feature which is composing the multimodal acquisition might be used for other searches in different single-trait databases in an unauthorized context.

The actuation of the previous guidelines is made difficult by the fact that some of them seem to appear as discordant or in mutual exclusion (*e.g.*, the third point can be in conflict to the fifth point), but some techniques available in the literature seem capable to effectively overcome these drawbacks.

As a matter of fact, the enhancements of the sensors and of the hardware/software architectures associated to the reduction of the system costs will produce a growing interest and diffusion of the multimodal systems in the market. The application of proper, practical and standard privacy-compliant guidelines is becoming more and more necessary.

1.5 AN EXEMPLIFYING SCHEME

Building over the considerations of the previous sections, we describe the design of a multimodal verification scheme satisfying much of the discussed issues regarding privacy compliance. The discussion will point out how few biometric traits might be used to construct an identification code for a subject while still ensuring protection to the biometric templates themselves. Also it will clarify a few problematic aspects which might be faced when constructing an actual implementation.

A typical multimodal biometric verification scheme provides two basic modules. The first, the *enroll* module, creates some sort of ID linked to a single user starting from the user's biometric samples. The ID could then be stored in *e.g.* a document or a smart card and must be provided during the verification phase. The second module, the *verification* one, verifies if the ID matches a new set of freshly provided biometrics.

While the number of biometric traits might in principle be increased as desired, we limit the discussion to the case of two independent biometric readings.

1.5.1 A multimodal enrollment module

At enrollment, as in common multimodal biometric systems, two different biometric readings are collected: *e.g.* an iris scan of one eye and a fingerprint or the fingerprints from two different fingers. The samples are then processed using the feature extraction algorithms of choice, selected among what the market or the open literature offer. Each algorithm delivers a set of features depending on the biometric trait, which are then turned into a binary string. For example, concerning fingerprints, the features describe characteristic points of the ridges' pattern; such numbers are then collected

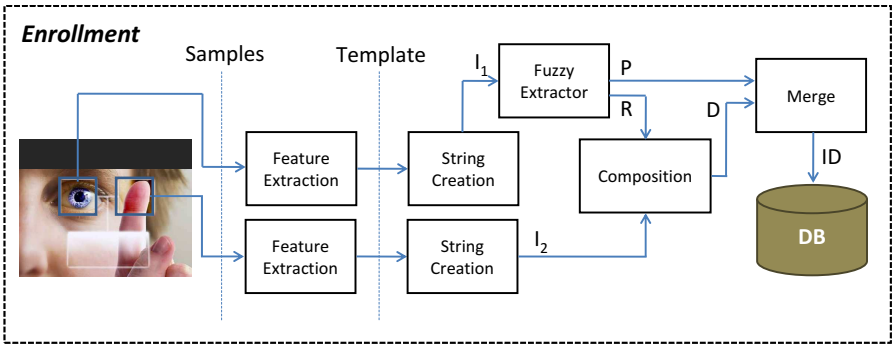

Fig. 1.3 A multimodal biometric enroll module satisfying privacy compliance issues.

in what is called a binary "template" possibly according to a standard. An example is the ANSI INCITS 378-2004 standard[1]. Similarly, for iris, the image of the eye is processed to obtained a string of bits (the so called "iris-code") directly.

In a simpler multimodal biometric system, the two templates denoted with I_1 and I_2 (Figure 1.3) would be stored in a database or a portable ID. An attacher who could somehow access the database or recover the ID might obtain with little effort the templates of the user. To avoid such scenario, the templates are generally encrypted using a public key infrastructure (thus relaying on *e.g.* a network). In here, following a different approach, the biometric strings are concealed exploiting their peculiar quality of being "similar" when obtained from the same subject.

The novelty with respect to a multimodal biometric system begins in figure 1.3 after the construction of I_1 and I_2. First, I_1 is fed into a "fuzzy extractor". Fuzzy extractors are cryptographic primitives which enable the extraction of a random uniform string R from a given input in a noise-tolerant way. Therefore they convert a noisy non-uniform input such as a biometric reading, into a easily and reliably reproducible binary string, allowing a certain degree of tolerance in the given input. The tolerance to variations within biometric strings is typically obtained using an $[n, k, 2t + 1]$ error correcting code, where n and k are the lengths of the codeword and the message respectively and t is the number of errors the code can correct. The code correcting capability t needs to be large enough to compensate for within-subject variability in the biometric samples. On the other hand it must be smaller that the between-subjects variability, or otherwise the tolerance of the fuzzy extractor might be so large that impostors might be recognized as genuine ID holders.

But this is actually not a big issue in practise. In fact usually the opposite problem arises and the error correcting capability of typical codes is not large enough for practical applications involving biometric samples. Given the large inter-subjects variability of biometric templates, the fraction of errors the code must be able to withstand is larger than in usual ECC applications. Common ECC code, like BCH,

[1] American National Standard for Information Technology X Finger Minutiae Format for Data Interchange.

are capable of correcting a fraction of errors n/t strictly $< 0.25\%$, thus are often ruled out[2]. Others binary codes might get closer to the $t/n = 1/2$ Singleton bound, but the Plotkin bound implies [13] that a binary code can correct more than $n/4$ errors only at the expenses of reducing the length of codeword to about $\log n$. This is the route one might pursue by deriving a binary code from a Reed-Solomon for which time-efficient decoding routines exist.

The fuzzy extractor produces two binary strings. The first, R must be kept secret while the second, P can be made public without disclosing any information on both I_1 and R. So, the scheme started with two "secrets", I_1 and I_2 and by now we only swapped the secret I_1 for R. But the important difference is that being R uniformly random by construction if we properly compose R and I_2 with a fuzzy commitment we are sure that no information is disclosed on both. Along this line a possible composition function might be the binary xor function.

The two string D and P, while derived from the biometrics provided by the subject at enrollment (and no other information) can not be used to obtain information on the biometric templates. They might be merged and published on an ID which the user could even safely lose.

1.5.1.1 A correspondent verification scheme The *verification* phase enables a "strong" authentication of the subject who has to provide both the biometric traits he was requested at enrollment and the ID he received. The overall structure is reported in figure 1.4.

The verification phase follows the line of a typical multimodal biometric verification. The subject is requested the same biometric traits he provided at enrollment and the samples are collected. From the samples, two fresh binary templates are constructed: I_1' and I_2'.

The fuzzy reconstructor guarantees that if the distance of I_1' from I_1 is within the tolerance of the error correcting code, and P is available (thus the ID is provided), the same secret R built at enrollment can be constructed (hence the name "reconstructor"). With R in hand, I_2 is easily decomposed from D. If the subject is an impostor the distance of its biometric sample and the ID holder one is larger than the fuzzy reconstructor tolerance and R is not reconstructed. The verification scheme is positively concluded if the retrieved biometric I_2 matches the fresh one I_2'.

In a biometric multimodal system with two inputs, we would have had two biometric comparisons. In the simple example we offered instead, the only biometric test is performed between I_2 and I_2' while the other enters the scheme through the fuzzy reconstructor only. While this is not an issue for biometric tests based only on Hamming distance measures (like in the case of iris-codes), it is the small price one needs to pay to enforce protection of the biometrics themselves.

[2]Actually, BCH codes could be employed in the schemes we suggested but the construction needs to be generalized slightly. The main idea is that injecting errors only over a restricted part of a longer codeword, a larger local error correction ratio is obtained; which in turn could easily satisfies the requirements imposed by the biometrics at hand.

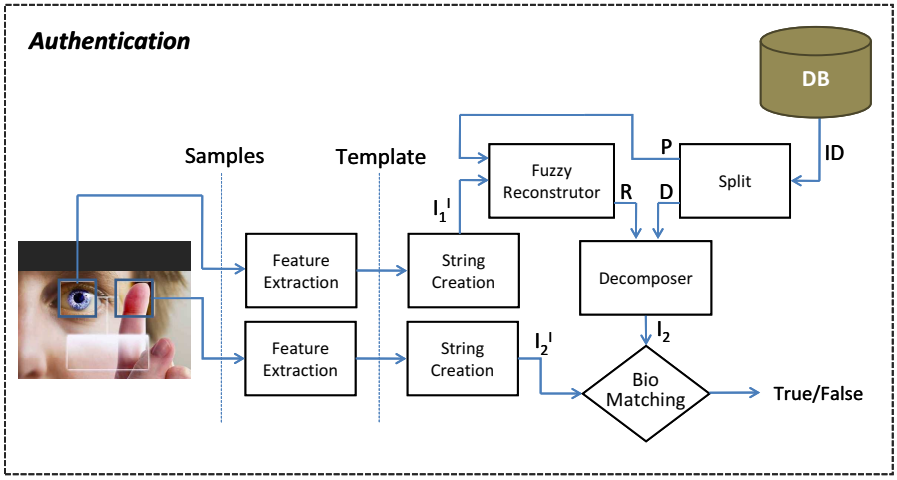

Fig. 1.4 A multimodal biometric verification module.

1.6 CONCLUSIONS

In this chapter we focused on issues and relative possible solutions regarding the privacy protection in the context of biometric systems. We described the risks perceived by the user approaching to biometric systems, and the actual risks for her/his privacy.

Privacy issues are pervasive in all the design phases of a biometric system: they can be related to the applicative context, to the approaches and goals set up when collecting the biometric data, and to the involved traits and technologies. Best practice notions have been discussed to ensure a privacy compliant design and management of biometric systems.

Recent advances show that it is possible to achieve an effective biometric template protection. Most techniques present in the literature are based on methods which combine standard cryptographic techniques and biometrics for the purpose of providing a privacy compliant and deployable identity verification system. The approaches we discussed are the fuzzy based constructions (Fuzzy Commitment, Fuzzy Vault, Fuzzy Sketch) and the hash based techniques. The application of these schemes offers a valid solution to the privacy protection of the user templates.

Multimodal systems revealed new privacy issues, and a set of guidelines for the design of a privacy-compliant system has been discussed. An exemplifying scheme is presented, showing a possible privacy compliant multimodal system. In particular, the proposed method is inherently multimodal: at least two biometric traits are simultaneously used to create a secure identifier. Such identifier combines the biometric features extracted in the enroll phase, ensuring that the verification phase can be correctly executed, but avoiding any attempt to mine the privacy of the users. Indeed, the information contained in the identifiers is not sufficient to reconstruct

the biometric features of the users and any abuse of biometric information is then prevented.

Moreover, the presented scheme satisfies the design guidelines. The security properties of the methods have been analyzed informally, and rely on the well investigated properties of the used fuzzy cryptographic primitives. The system is completely modular: both the input biometric readings and the matching procedures can be selected among the different ones proposed in the open literature. Composed systems can be constructed by assembling a number of enroll and verification modules requiring a corresponding larger number of input biometric readings, in order to achieve a higher degree of security when requested by the application.

REFERENCES

1. Russell Ang, Reihaneh Safavi-Naini, and Luke McAven. Cancelable key-based fingerprint templates. In *ACISP*, pages 242–252, 2005.

2. X. Boyen. Reusable cryptographic fuzzy extractors. In *11th ACM Conference on Computer and Communication Security (CCS 2004)*, volume 3027, pages 82–91. ACM, 2004.

3. X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith. Secure remote authentication using biometric data. In R. Cramer, editor, *Advances in Cryptology (EUROCRYPT 2005)*, volume 3494 of *Lecture Notes in Computer Science*. Springer-Verlag, 2005.

4. Julien Bringer, Hervé Chabanne, Gerad Cohen, Bruno Kindarji, and Gilles Zémor. Optimal iris fuzzy sketches. In *IEEE Conference on Biometrics: Theory, Applications and Systems (BTAS 07)*, 2007.

5. Society Centre for Science and Citizenship. Biometric identification technology ethic (bite project), 2006.

6. Ee-Chien Chang and Qiming Li. Hiding secret points amidst chaff. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 59–72. Springer, 2006.

7. T. Charles Clancy, Negar Kiyavash, and Dennis J. Lin. Secure smartcardbased fingerprint authentication. In *WBMA '03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, pages 45–52, New York, NY, USA, 2003. ACM.

8. Tee Connie, Andrew Teoh Beng Jin, Michael Goh Kah Ong, and David Ngo Chek Ling. Palmhashing: a novel approach for cancelable biometrics. *Inf. Process. Lett.*, 93(1):1–5, 2005.

9. J. G. Daugman. High confidence visual recognition of persons by a test of statistical indenpendence. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 15:1148–1161, 1993.

10. G. I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through off-line biometric. In *Proceedings of the IEEE International Symposium on Security and Privacy, 1998*, pages 148–157. IEEE Press, 1998.

11. G. I. Davida, Y. Frankel, B. J. Matt, and R. Peralta. On the relation of error correction and cryptography to an off line biometrics based identification scheme. In *WCC99, Workshop on Coding and Cryptography*, 1999.

12. Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Cristian Cachin and Jan Camenisch, editors, *Advances in Cryptology (EUROCRYPT 2004)*, volume 3027 of *Lecture Notes in Computer Science*. Springer-Verlag, 2004.

13. Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors. In P. Tuyls and J. Goseling, editors, *Security with Noisy Data*, chapter 5, pages 93–111. Springer-Verlag, 2007.

14. F. Hao, R. Anderson, and J. Daugman. Combining cryptography with biometrics effectively. Technical Report UCAM-CL-TR-640, University of Cambridge, Computer Laboratory, United Kingdom, July 2005.

15. K. Inman and N. Rudin. *An Introduction to Forensic DNA Analysis*. CRC press, Boca Raton, Florida, 1997.

16. LLC International Biometric Group. Bioprivacy initiative, 2003.

17. Pugh JA, Jacobson JM, Van Heuven WA, Watters JA, Tuley MR, Lairson DR, Lorimor RJ, Kapadia AS, and Velez R. Screening for diabetic retinopathy. the wide-angle retinal camera. *Diabetes Care*, 16(6):889–95, 1993.

18. A. K. Jain, A. Ross, and S. Pankanti. Biometrics: A tool for information security. *IEEE transactions on information forensics and security*, 1(2):125–143, June 2006.

19. Anil K. Jain, Salil Prabhakar, Lin Hong, and Sharath Pankanti. Filterbank-based fingerprint matching. *IEEE Transactions on Image Processing*, 9(5):846–859, 2000.

20. A. Teoh Beng Jin, D. Ngo Chek Ling, and A. Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 37(11):2245–2255, 2004.

21. Andrew Teoh Beng Jin, David Ngo Chek Ling, and Alwyn Goh. Personalised cryptographic key generation based on facehashing. *Computers & Security*, 23(7):606–614, 2004.

22. A. Juels and M. Sudan. A fuzzy vault scheme. In A. Lapidoth and E. Teletar, editors, *Proceedings of the IEEE International Symposium on Information Theory, 2002*, page 408. IEEE Press, 2002. The full version of the paper is located at http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/fuzzy-vault/fuzzy_vault.pdf.

23. Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *CCS '99: Proceedings of the 6th ACM conference on Computer and communications security*, pages 28–36, New York, NY, USA, 1999. ACM Press.

24. Tom A. M. Kevenaar, Geert Jan Schrijen, Michiel van der Veen, Anton H. M. Akkermans, and Fei Zuo. Face recognition with renewable and privacy preserving binary templates. In *AutoID*, pages 21–26, 2005.

25. L. Nanni and A. Lumini. Empirical tests on biohashing. *NeuroComputing*, 69(16):2390–2395, October 2006.

26. S. Prabhakar, S. Pankanti, and A.K. Jain. Biometric recognition: Security & privacy concerns. *IEEE Security & Privacy Magazine*, 1(2):33–42, March-April 2003.

27. Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, and Ruud M. Bolle. Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4):561–572, 2007.

28. Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

29. B. Schneier. Biometrics: uses and abuses. *Commun. ACM*, 42(8):136, August 1999.

30. D. Schonberg and D. Kirovski. Eyecerts. *IEEE Transactions on Information Forensics and Security*, 1:144–153, June 2006.

31. R. Snelick, U. Uludag, A. Mink, M. Indovina, and A.K. Jain. Large scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 27(3):450–455, March 2005.

32. Yagiz Sutcu, Qiming Li, and Nasir Memon. Protecting biometric templates with sketch: Theory and practice. *IEEE Transaction on Information Forensics and Security*, 2(3), 2007.

33. Valérie Viet Triem Tong, Hervé Sibert, Jérémy Lecoeur, and Marc Girault. Biometric fuzzy extractors made practical: A proposal based on fingercodes. In *ICB*, pages 604–613, 2007.

34. Pim Tuyls, B. Skoric, and T. Kevenaar, editors. *Security with Noisy Data*. Springer, 2008.

35. U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain. Biometric cryptosystems: Issues and challenges. In *Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management*, volume 92, pages 948–960, June 2004.

36. Umut Uludag, Sharath Pankanti, and Anil K. Jain. Fuzzy vault for fingerprints. In Takeo Kanade, Anil K. Jain, and Nalini K. Ratha, editors, *AVBPA*, volume 3546 of *Lecture Notes in Computer Science*, pages 310–319. Springer, 2005.

37. Claus Vielhauer, Ralf Steinmetz, and Astrid Mayerhöfer. Biometric hash based on statistical features of online signatures. In *ICPR (1)*, pages 123–126, 2002.