Chapter 8

Multi-Biometric Template Protection: Issues and Challenges

Christian Rathgeb and Christoph Busch

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/52152

1. Introduction

The term biometrics refers to "automated recognition of individuals based on their behavioral and biological characteristics" (ISO/IEC JTC1 SC37). Several physiological (static) as well as behavioral (non-static) biometric characteristics have been exploited [1] such as fingerprints, iris, face, hand, voice, gait, keystroke dynamics, etc., depending on distinct types of applications (see Figure 1). Biometric traits are acquired applying adequate sensors and distinctive feature extractors are utilized in order to generate a biometric template (reference data) in the enrollment process. During verification (authentication process) or identification (identification can be handled as a sequence of biometric comparisons against the enrollment records in a reference databse) the system processes another biometric measurement from which an according template is extracted and compared against the stored template(s) yielding acceptance/ rejection or hit/ no-hit, respectively.

The presented work is motivated by very recent advances in the fields of *multi-biometric recognition* [2] and *biometric template protection* [3]. Automatic recognition systems based on a single biometric indicator often have to contend with unacceptable error rates [4]. Multi-biometric systems have improved the accuracy and reliability of biometric systems [2]. Biometric vendors are already deploying multi-biometric systems (e.g. fingerprint and finger vein by SAFRAN Morpho[1]) and multi-biometric recognition is performed on large-scale datasets (e.g. within the Aadhaar project [5] by the Unique Identification Authority of India (UIDAI)). However, security of multi-biometric templates is especially crucial as they contain information regarding multiple traits of the same subject [6]. The leakage of any kind of template information to unauthorized individuals constitutes serious security and privacy risks, e.g. permanent tracking of subjects without consent [7] or reconstruction of original biometric traits (e.g. fingerprints [8] or iris textures [9]) might become a realistic threat. Therefore, biometric template protection technologies have been developed in order to protect privacy and integrity of stored biometric data. However, so far, template protection schemes which provide provable security/ privacy, and achieve practical recognition rates

[1] SAFRAN Morpho, France, http://www.morpho.com/

(a) Iris (b) Fingerprint (c) Face (d) Palmprint

Figure 1. Examples of physiological (static) biometric characteristics.

have remained elusive, even on small datasets. This bookchapter provides a comprehensive overview of biometric fusion, biometric template protection, and, in particular, possible ways of how to combine these technologies.

The remainder of this bookchapter is organized as follows: Section 2 briefly summarizes advantages and issues of multi-biometric recognition. Template protection technologies are reviewed in Section 3. In Section 4 multi-biometrics and template protection are combined and related works are summarized. Subsequently, a theoretical framework for multi-biometric template protection is introduced and major issues and challenges evolving from incorporating biometric fusion to template protection technologies are discussed in detail in Section 5. Finally, a summary is given in Section 6.

2. Multi-biometric recognition

Whenever biometric verification systems based on single biometric indicators have to deal with noisy sensor acquisition, restricted degrees-of-freedom, or non-universality unpractical performance rates are yielded [4]. Such drawbacks, which represent common scenarios when operating biometric recognition systems, raise the need for multi-biometric recognition [2] or other approaches that can increase the recognition accuracy. As previously mentioned, a fusion of multiple biometric indicators have been shown to improved the accuracy and reliability of biometric systems.

2.1. Categorization

Fusion in biometric systems is commonly categorized according to the level within which the fusion is performed. ISO/IEC TR 24722:2007 coarsely distinguishes three possible levels of fusion: (1) fusion at feature level, (2) fusion at score level, and (3) fusion at decision level. Figure 2 illustrates these different types of biometric fusion.

1. *Feature Level Fusion*: biometric fusion on feature level comprises the construction of a new feature vector of higher dimensionality composed of (a selection of) feature elements of various feature vectors generated a priori. The new feature vector should turn out to be more discriminative than each single one [4].
2. *Score Level Fusion*: on this level of fusion matching scores are returned by each individual subsystem and obtained scores are combined. Once scores are properly normalized they can be combined in different ways (e.g. by weighted sum-rule) such that the fusion of normalized scores leads to a more accurate overall system.

http://dx.doi.org/10.5772/52152

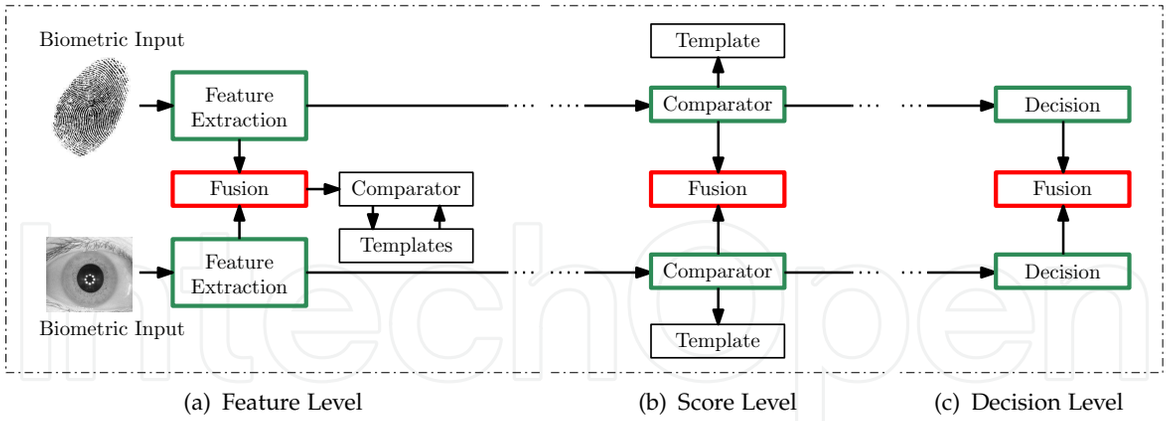


Figure 2. Biometric fusion: different levels of fusion within a biometric recognition system.

3. *Decision Level Fusion*: a fusion of final decisions (in general accept/ reject) is referred to as decision level fusion. Various final decisions of independent subsystems can be fused (e.g. by applying a majority voting) in order to increase the accuracy (security) or universality (convenience) of the entire system [2].

2.2. Advantages

Multi-biometric recognition systems offer several advantages compared to conventional biometric systems. There is a common and intuitive assumption that the combination of multiple biometrics improves performance as multiple multiple sources of information are involved. By combining multiple sources of information, it is possible to improve systems biometric performance, increase population coverage, deter spoofing, and facilitate indexing [10]. While several fusion levels are possible in multi-biometric systems (see Chapter 2.1), biometric fusion on the score level represents the most popular one due to the ease in accessing and consolidating comparison scores. Performance gain is achieved in case uncorrelated traits are applied in a multi-biometric recognition systems. Incorporating subject-specific parameters may further increase accuracy of these systems.

However, in case a strong (highly discriminative) biometric characteristic is combined with a weak one, the resulting decision environment is in a sense averaged, and the combined performance will lie somewhere between that of the two tests conducted individually. Hence, biometric fusion is not straight forward, but highly depends on the choice of characteristics, features, fusion type, etc.

2.3. Issues

Besides common issues like requirements for stronger user incorporation of feature level fusion of different feature representations, one major issue regarding multi-biometric recognition we want to emphasize on is the central storage of multiple biometric templates of a single subject. Compared to conventional biometric systems based on a single biometric indicator, multiple sources of information, i.e. more biometric reference data, has to be stored for each subject registered with a multi-biometric system. In a multi-biometric system the overall complexity increases as multiple SDK need to be maintained and the use of multiple

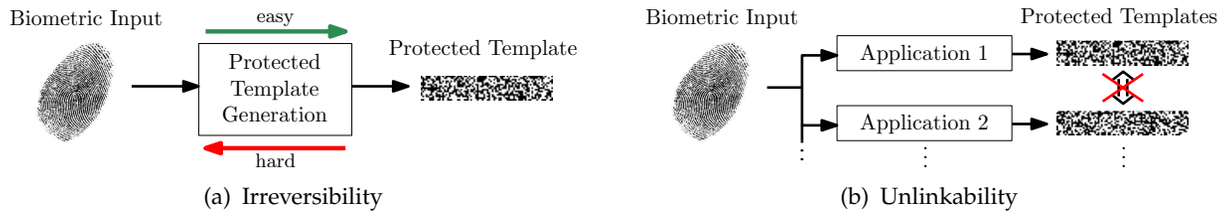


Figure 3. Biometric template protection: properties of (a) irreversibility and (b) unlinkability.

sensors results in a stronger dependency on fully operational hardware. Biometric system can be compromised in a number of ways [7], and leakage of biometric template information to unauthorized individuals constitutes serious security and privacy threats [6]. For instance, in case n different comparison scores are combined performing score level fusion, n different biometric templates have to be stored for each subject registered with the system.

This major drawback of biometric fusion raises the need for multi-biometric template protection. More precisely, the storage of multiple biometric records of a fused template of biometric features extracted from different biometric traits has to be protected.

3. Template protection

The industry has long claimed that one of the primary benefits of biometric templates is that original biometric signals acquired to enroll a data subject cannot be reconstructed from stored templates. Several techniques (e.g. [8, 11]) have proven this claim wrong. Since most biometric characteristics are largely immutable, a compromise of raw biometric data or biometric templates might result in a situation that a subject's biometric characteristics are essentially *burned* and not usable any longer from the security perspective. Biometric template protection technologies offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at a high security level.

3.1. Categorization

Biometric template protection schemes are commonly categorized as (1) biometric cryptosystems (also referred to as helper data-based schemes) and (2) cancelable biometrics (also referred to as feature transformation). Biometric cryptosystems are designed to securely bind a digital key to a biometric or generate a digital key from a biometric [12], offering solutions to biometric-dependent key-release and biometric template protection [13, 14]. Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transforms which provide a comparison of biometric templates in the transformed domain [7]. Both technologies are designed to meet two major requirements of biometric information protection (ISO/IEC 24745): (1) *irreversibility*, i.e. it should be computationally hard to reconstruct the original biometric template from the stored reference data (protected template), while it should be easy to generate the protected biometric template; (2) *unlinkability*, i.e. different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching (diversity). Schematic illustrations of both properties are shown in Figure 3(a) and Figure 3(b).

http://dx.doi.org/10.5772/52152

Advantage	Description
Privacy protection	Within biometric cryptosystems and cancelable biometrics the original biometric template is obscured such that a reconstruction is hardly feasible.
Secure key release	Biometric cryptosystems provide key release mechanisms based on biometrics.
Pseudonymous authentication	Authentication is performed in the encrypted domain and, thus, the biometric reference is a pseudonymous identifier.
Revocability and renewability of templates	Several instances of secured templates can be generated.
Increased security	Biometric cryptosystems and cancelable biometrics prevent from several traditional attacks against biometric systems.
More social acceptance	Biometric cryptosystems and cancelable biometrics are expected to increase the social acceptance of biometric applications.

Table 1. Major advantages of technologies of biometric template protection.

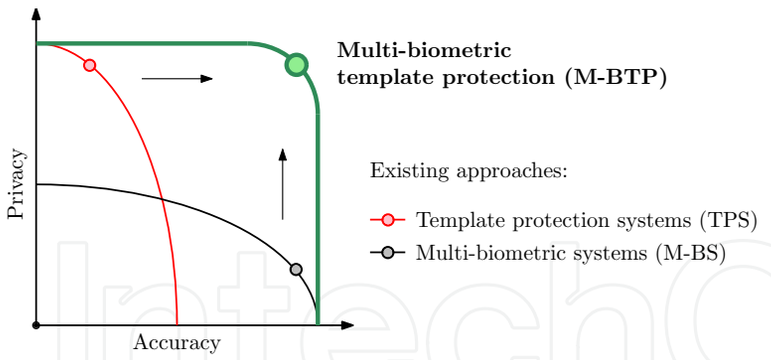
3.2. Advantages

Biometric cryptosystems and cancelable biometrics offer several advantages over generic biometric systems. Most important advantages are summarized in Table 1. These major advantages over conventional biometric systems call for several applications. In order to underline the potential of both technologies two essential use cases are discussed in detail. With respect to the design goals, biometric cryptosystems and cancelable biometrics offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at an high security level. Several new issues and challenges arise deploying these technologies [13].

3.3. Issues

One fundamental challenge, regarding template protection, represents the issue of alignment, which significantly effects recognition performance. Biometric templates are obscured within both technologies, i.e. alignment of obscured templates without leakage is highly non-trivial. For instance, if iris biometric textures or templates (iris-codes) are transformed in a non-row-wise manner, e.g. block permutation of preprocessed textures or a permutation of iris-code bits. Consequentially, additional information, which must not lead to template reconstruction, has to be stored [3].

Focusing on biometric template protection technologies it is not actually clear which biometric characteristics to apply in which type of application. In fact it has been shown that even the iris may not exhibit enough reliable information to bind or extract sufficiently long keys providing acceptable trade-offs between accuracy and security. Stability of biometric features is required to limit information leakage of stored helper data. In addition, feature adaptation schemes that preserve accuracy have to be utilized in order to obtain common representations of arbitrary biometric characteristics (several approaches to extract fixed-length binary fingerprint templates have been proposed, e.g. [15, 16]).



System	Privacy	Accuracy
TPS	high	low
M-BS	low	high
M-BTP	high	high

Figure 4. Privacy/ accuracy relation: multi-biometrics and template protection systems.

As plenty different approaches to biometric cryptosystems and cancelable biometrics have been proposed a large number of pseudonyms and acronyms have been dispersed across literature such that attempts to represented biometric template protection schemes in unified architectures have been made [17]. Standardization on biometric template protection has been achieved in the ISO/IEC 24745 standard providing guidance on the protection of an individual's privacy during the processing of biometric information.

4. Multi-biometric template protection

As previously mentioned, a lack of security represents a major drawback of multi-biometric recognition systems [6]. On the other hand, biometric template protection technologies generally reveal unpractical accuracy compared to underlying recognition algorithms [3]. These facts motivate the incorporation of template protection technologies to multi-biometric recognition systems, and vice versa.

4.1. Combining the best of two worlds

With respect to the described design goals, i.e. *breaking the trade-off* between accuracy and security, multi-biometric template protection systems offer significant advantages, improving public confidence and acceptance of biometrics. In addition, multi-biometrics provide low error rates compared to uni-biometric systems even under unconstrained circumstances paving the way for practical deployment of template protection systems. The relation between approaches to multi-biometric recognition and biometric template protection is schematically illustrated in Figure 4, highlighting the potential of multi-biometric template protection.

4.2. Related work

Focusing on the current state-of-the-art in biometric template protection key approaches to biometric cryptosystems and cancelable biometrics are summarized in Table 2. Representing one of the simplest key binding approaches the fuzzy commitment scheme [18] has been successfully applied to iris [19] (and other biometrics). The fuzzy vault scheme [20] which represents one of the most popular biometric cryptosystem has frequently been applied to fingerprints. Early approaches (e.g. [21]), which required a pre-alignment of biometric templates, have demonstrated the potential of this concept. Several techniques (e.g. [22, 23]) to overcome the shortcoming of pre-alignment have been proposed. Quantization schemes

http://dx.doi.org/10.5772/52152

Author(s)	Applied Technique	Modality	FRR / FAR (%)	Remarks
[19]	Fuzzy Commitment	Iris	0.42 / 0.0	small test set
[34]			5.62 / 0.0	short key
[21]	Fuzzy Vault	Fingerprints	20-30 / 0.0	pre-alignment, >1 enroll sam.
[23]			4.0 / 0.004	>1 enroll sam.
[35]		Iris	5.5 / 0.0	–
[36]	Quantization	Online Sig.	28.0 / 1.2	>1 enroll sam.
[24]			7.05 / 0.0	short key
[26]	Password-Hardening	Voice	>2.0 / 2.0	short key
[37]	BioHashing	Face	0.0 / 0.0	non-stolen token
[38]	Block Permutation, Surface Folding	Fingerprints	$\sim$35 / 10^{-4} $\sim$15 / 10^{-4}	–
[39]	BioConvolving	Online Sig.	10.81 EER	–
[33]	BioHashing	Face	0.0002 EER	non-stolen token

Table 2. Experimental results of key approaches to biometric template protection schemes.

(e.g. [24, 25]) have been applied to several physiological and behavioral biometrics, while focusing on reported performance rates, these schemes require further studies in order to improve accuracy. Besides, approaches which aim at "salting" existing passwords with biometric features have been proposed [26]. Within the BioHashing approach [27] biometric features are projected onto secret domains applying user-specific tokens prior to a key-binding process. Variants of this approach have been exposed to reveal unpractical performance rates under the stolen-token scenario [28]. With respect to recognition rates, the vast majority of biometric template protection schemes are by no means comparable to conventional biometric systems. While numerous approaches to biometric cryptosystems generate rather short keys at unacceptable performance rates, several enrollment samples may be required as well, (e.g. four samples in [21]). Approaches which report practical recognition rates are tested on rather small datasets (e.g. 70 persons in [19]) which must not be interpreted as significant. In addition, the introduction of additional tokens, be it random numbers or secret PINs, often clouds the picture of reported results.

First approaches to non-invertible transforms [7] (representing an instance of cancelable biometrics), which have been applied to face and fingerprints, include block-permutation and surface-folding. Diverse proposals (e.g. [29, 30]) have shown that recognition performance decreases noticeably compared to original biometric systems. Additionally, it is doubtable if sample images of transformed biometric images are non-invertible. BioHashing [27] (without key-binding) represents the most popular instance of biometric salting yielding a two-factor authentication scheme. Since additional tokens have to be kept secret (e.g. [31, 32]) result reporting turns out to be problematic. Perfect recognition rates have been reported (e.g. in [33]) while the opposite was found to be true [28] within the stolen-token scenario.

Focusing on the incorporation of multiple biometrics in template protection schemes several approaches have been proposed. Most notable approaches are summarized in Table 3. One of the first approach to a multi-biometric cryptosystem based on the fuzzy commitment scheme was proposed by [40], in which binary fingerprint and face features are combined. In [41] two different feature extraction algorithms are applied to 3D face data yielding a single

Author(s)	Applied Technique	Modality	FRR / FAR (%)	Remarks
[40]	Multi-biometric Fuzzy Commitment	Fingerprint and Face	0.92 / >0.001	–
[41]		3D Face and 3D Face	∼ 2.5 EER	single sensor scenario
[42]		Iris and Iris	5.56 / 0.01	single sensor scenario
[43]	Multi-biometric Fuzzy Vault	Fingerprint and Iris	1.8 / 0.01	–
[6]		Fingerprint, Face and Iris	1.0 / 0.0	–
[44]	Token-based Scrambling	Face and Face	∼ 15.0 EER	single sensor scenario

Table 3. Experimental results of approaches to multi-biometric template protection schemes.

sensor scenario[2]. The authors provide results for feature level, score level and decision level fusion. In order to obtain a comparison score the number of errors corrected by the error correction code are estimated, i.e. scores are only available in case of successful decoding. Best results are obtained for the multi-algorithm fusion at feature level. [42] propose a sensible rearrangement of bits in iris codes in order to provide a uniform distribution of error probabilities. The rearrangement allows a more efficient execution of error correction codes combining the most reliable bits generated by different feature extraction algorithms. [43] proposed a multi-biometric cryptosystem fuzzy vault based on fingerprint and iris. The authors demonstrate that a combination of biometric modalities leads to increased accuracy and, thus, higher security. A FRR of 1.8% at a FAR of ∼0.01% is obtained, while the corresponding FRR values of the iris and fingerprint fuzzy vaults are 12% and 21.2%, respectively. [44] combine two different feature extraction methods to achieve cancelable face biometrics. PCA and ICA (independent component analysis) coefficients are extracted and both feature vectors are randomly scrambled and added in order to create a transformed template. In rather recent work [6] report results on multi-biometric fuzzy commitment schemes and fuzzy vault schemes based on fingerprint, face and iris. In order to obtain a common feature representation for each type of template protection scheme the authors propose different embedding algorithms, e.g. for mapping a binary string to a point set. best results are obtained for a multi-biometric fuzzy vault scheme. Compared to feature level fusion and score level fusion, recently [45] proposed a multi-biometric template protection system employing decision level fusion of multiple protected fingerprint templates.

Several other ideas of using a set of multiple biometric characteristics within biometric template protections schemes have been proposed [46–51].

[2] Note that in general single sensor scenarios are more challenging than those based on multiple sensors, since, in case of noise occurrence, each feature extractor has to deal with signal degradation.

http://dx.doi.org/10.5772/52152

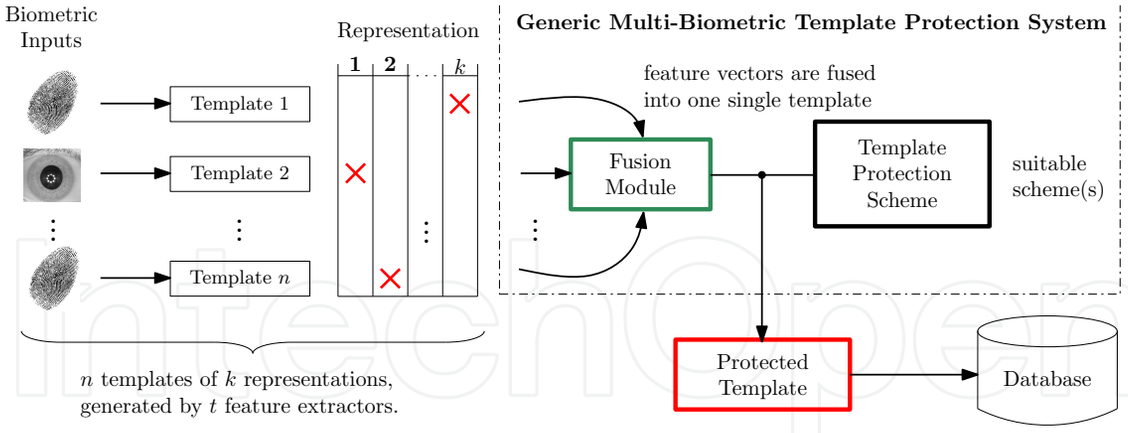


Figure 5. A framework of a generic multi-biometric template protection at feature level.

That is, a rearrangement of biometric feature vectors in order to provide a uniform distribution of errors improves the overall accuracy of the system.

5. Issues and challenges

Besides already mentioned issues of multi-biometric recognition (see Chapter 2.3) and template protection technologies (see Chapter 3.3), which may be solved through multi-biometric template protection, several further issues might occur which have to be dealt with. From designing a generic framework for multi-biometric template protection at a coarse level different evolving issues will be discussed in detail.

5.1. Generic framework for multi-biometric template protection

The major goal of research in the area of multi-biometric template protection is to generate a *generic framework* of constructing multi-biometric template protection schemes, i.e. a code of practice according to various aspects for incorporating different biometric templates in one or more template protection system(s), yielding multi-biometric template protection. From existing research it appears that biometric fusion on feature level is most suitable for template protection schemes [6, 40–42]. While preliminary scores are not available within the vast majority of biometric cryptosystems, cancelable biometric systems based on score level fusion can be constructed analogue to conventional biometric systems. For both technologies biometric fusion based on decision level can easily be implemented combining final decisions. Figure 5 shows a schematic impression of how such a framework (based on feature level fusion) could look like.

In order to provide generic multi-biometric template protection the system should be capable of incorporating n different biometric templates, which need not exhibit a common feature representation, i.e. k different representation may be involved. In a fusion module a common representation of feature vectors is established and feature vectors are combined in a sensible manner. Subsequently, an adequate template protection scheme is applied to protect the multi-biometric template. Focusing on a generic fusion of multiple biometric templates in a template protection system several issues evolve.

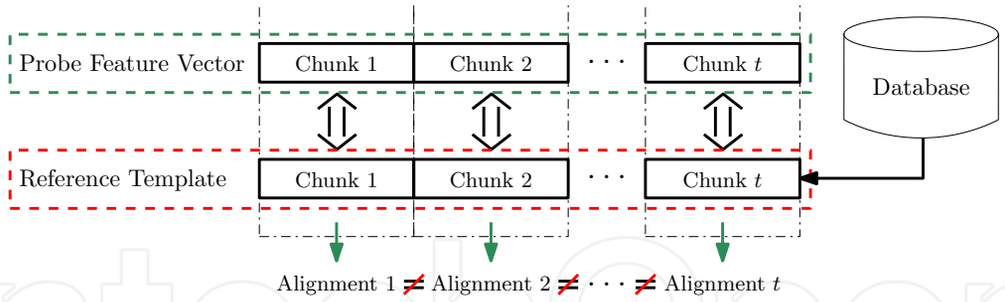


Figure 6. Template alignment within a multi-biometric template protection scheme.

5.2. Template alignment

Focusing on distinct biometric characteristics, e.g. iris, alignment within a template protection scheme can still be feasible. For instance, within an iris biometric fuzzy commitment scheme template alignment can be achieved by applying decommitments at various shifting positions. Within conventional biometric systems align-invariant approaches have been proposed for several biometric characteristics. So far, hardly any suggestions have been made to construct align-invariant biometric cryptosystems or cancelable biometrics. Still, focusing on technologies of biometric template protection, feature alignment significantly effects recognition performance. Biometric templates are obscured within template protection systems, i.e. alignment of protected templates is highly non-trivial [52]. Feature level fusion of biometric templates potentially aggravates a proper alignment of protected templates (optimal alignments vary for incorporated templates), while auxiliary data for the use of alignment may leak information on stored templates. More precisely, a combined feature vector may consist of t chunks of feature elements generated by t diverse feature extractors. In order to establish a proper alignment of the entire feature vector, chunks of feature elements need to be aligned individually. In general a common optimal alignment which is valid for all chunks of feature elements is rather unlikely. Hence, additional helper data is required which at least has to mark start and end points of such chunks. Figure 6 provides an schematic illustration of this issue.

As previously mentioned an adaption of biometric feature vectors to template protection schemes is considered inevitable in order to achieve practical recognition rates. However, generally a rearrangement of features within biometric templates makes conventional template alignment infeasible. Again, in order to align protected templates properly, additional helper data (e.g. reverse permutations) need to be stored (cf. [22, 23]), in a global or subject-specific manner. The additional storage of helper data is essential but will cause information leakage, i.e. potential impostors may utilize the additional helper data in order to compromise or cross-match protected templates, in case of subject-specific helper data.

5.3. Combination of modalities

In fact it has been shown that distinct biometric modalities (e.g. fingerprint or iris) exhibit enough reliable information to bind or extract sufficiently long keys providing acceptable trade-offs between accuracy and security, where the best performing schemes are based on fuzzy commitment and fuzzy vault. However, practical error correction codes are designed for communication and data storage purposes such that a perfect error correction code for a desired code length has remained evasive (optimal codes exist only theoretically under

http://dx.doi.org/10.5772/52152

certain assumptions [53]). The fact that false rejection rates are lower bounded by error correction capacities [54] emerges a great challenge since unbounded use of error correction (if applicable) makes the system even more vulnerable [55]. Other characteristics such as voice or keystroke dynamics (especially behavioral characteristics) were found to reveal only a small amount of stable information [26], but can still be applied to improve the security of an existing secret. While for some characteristics extracting of a sufficient amount of reliable features seems to be feasible it still remains questionable if these features exhibit enough entropy. In case extracted features do not meet requirements of discriminativity, systems become vulnerable to several attacks (e.g. false acceptance attacks). In addition, stability of biometric features is required to limit information leakage of stored helper data as well as a sufficient secret length. Focusing on multi-biometric template protection schemes which perform biometric fusion at feature level a single sensor fusion scenario could be applied in order to overcome the issue of alignment. Any combination of biometric feature vectors extracted from a single biometric signal alleviates the construction of a multi-biometric template protection scheme, in case these feature extractors apply the same mode of operation when analyzing biometric data. For instance, if two different iris biometric feature extractors extract binary iris-codes from pre-processed textures and operate on same block sizes extracting the same number of bits per block, a single optimal alignment for both extracted feature vectors exists.

Due to the sensitivity of template protection schemes multiple enrollment samples are required and thus, compared to conventional biometric systems, more user-cooperation (compared to conventional biometric systems) is demanded in order to decrease intra-class variation, while sensoring and preprocessing require improvement as well. Furthermore, from the usability side of view it has to be analyzed which combinations of biometric modalities are applicable (e.g. iris and face or fingerprint and hand geometry) [2]. In order to keep the multi-biometric system usable only those modalities should be combined that allow acquisition of multiple samples with "one" single capture device (e.g. capturing two iris images and one face image with multiple cameras that are integrated in one capture device). Only then the capture time and consequently the transaction time will remain constant.

5.4. Feature representation

While different template protection systems incorporating multiple biometric traits have been proposed, these turn out to be custom-built according to applied biometric feature representations and applied template protection schemes. Multi-biometric template protection schemes in literature have been proposed for numerous types of template protection requiring different feature representations (a detailed overview can be found in [3]). While some techniques have been applied to distinct template protection systems (e.g. fuzzy commitment scheme or fuzzy vault scheme) a detailed analysis of pros and cons of these schemes regarding the application of multi-biometrics has remained elusive. Such investigation involves factors such as scalability, i.e. the vast majority of template protection schemes require fixed-length feature vectors and are only scalable in discrete iterations (e.g. by adding a distinct number of chunks of error correction codewords). Biometric template protection schemes are designed for a distinct representation of feature vectors, e.g. fuzzy commitment schemes require binary biometric templates as input while fuzzy vault schemes require real-valued biometric templates. A fusion of binary iris-codes and

minutiae triples can still be performed without a successive application of different types of template protection schemes (e.g. in [43]). However, as this is not the case in general, embedding functions are required in order to perform mappings between different feature representations; such mappings must not cause a drastic loss of information.

Since different template protection schemes require distinct feature representations a generic framework for multi-biometric template protection should be able to handle diverse inputs of feature vectors. This issue can be solve in two ways:

1. *Unified representation*: by establishing a common representation of biometric features (e.g. by quantizing feature vectors [24]) or
2. *Different template protection schemes*: by combining different types of template protection schemes according to the provided feature vectors (e.g. fuzzy commitment scheme and fuzzy vault scheme [43]).

It is expected that the first opportunity degrades discriminativity of feature vectors while the second is expected to cause security vulnerabilities of protected templates. In order to prevent impostors from attacking separately stored protected templates biometric fusion can be performed at "secret level", i.e. each applied template protection scheme contributed a chunk of bits while the final secret is constructed from calculating a hash of the concatenation of all bit chunks. Still, representation of feature vectors represents one of the most critical issues.

5.5. System security

Focusing on the possible levels of fusion existing approaches to feature-level fusion in template protection systems merely involve a trivial concatenation of biometric templates (e.g. [40, 41]). It has been demonstrated, to some extent, that a more-sophisticated feature-level fusion leads to improved accuracy as well as template security [42]. However, more detailed analysis of adapting multiple biometric templates (based on different feature representations) to according template protection schemes on feature level is demanded. While approaches to cancelable biometrics provide a comparison score for each authentication attempt (offering trivial score-level fusion), within biometric cryptosystems subjects are authenticated indirectly via key validities, i.e. comparison scores are not explicitly available. For instance, in [41] comparison scores are equalized with required error correction capacities, however, more sophisticated approaches to multi-biometric cryptosystems based on score level fusion are non-existent. Biometric fusion at decision level implies the incorporation of a significant amount of biometric templates (e.g. to enable majority voting) in a template protection system. For both technologies, biometric cryptosystems and cancelable biometrics, biometric fusion on decision level can be implemented straight-forward. With respect to biometric cryptosystems a way of performing biometric fusion on secret level could be implemented by a (bit-wise) majority vote of released keys. Even tough approaches to cancelable biometric may easily be fused at decision level, recognition performance does not necessarily correlate with results reported for traditional multi-biometric systems. However, by definition, this level of fusion is restricting the system to a separate protection of multiple templates, which need to be secured individually, and can cause further security risks [6].

http://dx.doi.org/10.5772/52152

In the vast majority of approaches to biometric template protection schemes provided security is put on a level with obtained recognition performance, i.e. obtained FAR at a targeted FRR. While analysis with respect to irreversibility and unlinkability is rarely done, some quantities to measure the security of template protection systems have been suggested, e.g. key entropy [56], maximum key size [57], or information leakage of stored helper data [58, 59]. These analysis need to be adapted and extended in order to establish a generic methodology of measuring the security of multi-biometric template protection systems.

Focusing on security/ privacy of template protection schemes several magnitudes have been proposed for uni-biometric template protection schemes (e.g. [56, 58]). With respect to multi-biometric template protection schemes security measures need to be reformulated and extended since additional factors, such as a separate storage of protected templates, take influence on the security provided by the system [6]. We plan to establish a generic modus operandi of estimating the security of any multi-biometric template protection scheme in an information theoretic way. Emphasis will also be put on irreversibility and unlinkability analysis, which is rarely done in existing literature (e.g. in [39]).

6. Summary

The presented bookchapter provides an overview of multi-biometric template protection. While both technologies, multi-biometric recognition [2] and biometric template protection [3], suffer from serious drawbacks a sensible combination of these could eliminate individual disadvantages. Different template protection systems incorporating multiple biometric traits, which have been proposed in literature, are summarized. While, at first glance, multi-biometric template protection seems to solve several drawbacks, diverse issues arise. Based on a theoretical framework for multi-biometric template protection several issues, e.g. template alignment at feature level, are elaborated and discussed in detail. While generic approaches to the construction of multi-biometric template protection schemes have remained elusive we provide several suggestions for designing multi-biometric template protection systems.

Acknowledgement

This work has been supported by the Center for Advanced Security Research Darmstadt (CASED).

Author details

Christian Rathgeb* and Christoph Busch

* Address all correspondence to: christian.rathgeb@cased.de

da/sec – Biometrics and Internet Security Research Group, Hochschule Darmstadt, Darmstadt, Germany

7. References

[1] A. K. Jain, P. J. Flynn, and A. A. Ross. *Handbook of Biometrics*. Springer-Verlag, 2008.

[2] A. Ross, K. Nandakumar, and A. K. Jain. *Handbook of Multibiometrics (International Series on Biometrics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[3] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*, 2011(3), 2011.

[4] A. Ross and A. K. Jain. Information fusion in biometrics. *Pattern Recognition Letters*, 24:2115–2125, 2003.

[5] Unique Identification Authority of India. Aadhaar, 2012. retrieved May, 2012.

[6] A. Nagar, K. Nandakumar, and A. K. Jain. Multibiometric cryptosystems based on feature level fusion. *IEEE Transactions on Information Forensics and Security*, 7(1):255–268, 2012.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40:614–634, 2001.

[8] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9):1489–1503, 2007.

[9] S. Venugopalan and M. Savvides. How to generate spoofed irises from an iris code template. *Trans. Information Forensics and Security*, 6:385–395, 2011.

[10] A. Ross and A. K. Jain. Multimodal biometrics: An overview. In *Proc. of 12th European Signal Processing Conf. (EUSIPCO'04)*, pages 1221–1224, 2004.

[11] Arun Ross, Jidnya Shah, and Anil K. Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544–560, 2007.

[12] A. Cavoukian and A. Stoianov. Biometric encryption. In *Encyclopedia of Biometrics*. Springer Verlag, 2009.

[13] A. Cavoukian and A. Stoianov. Biometric encryption: The new breed of untraceable biometrics. In *Biometrics: fundamentals, theory, and systems*. Wiley, 2009.

[14] A. K. Jain, A. Ross, and U. Uludag. Biometric template security: Challenges and solutions. *in Proc. of European Signal Processing Conf. (EUSIPCO)*, 2005.

[15] J. Bringer and V. Despiegel. Binary feature vector fingerprint representation from minutiae vicinities. In *Proc. of the 4th IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'10)*, pages 1–6, 2010.

[16] H. Xu and R. N.J. Veldhuis. Binary representations of fingerprint spectral minutiae features. In *Proc. of the 20th Int. Conf. on Pattern Recognition (ICPR'10)*, pages 1212–1216, 2010.

[17] J. Breebaart, C. Busch, J. Grave, and E. Kindt. A reference architecture for biometric template protection based on pseudo identities. In *Proc. of the BIOSIG 2008: Biometrics and Electronic Signatures*, pages 25–38, 2008.

[18] A. Juels and M. Wattenberg. A fuzzy commitment scheme. *6th ACM Conf. on Computer and Communications Security*, pages 28–36, 1999.

[19] F. Hao, R. Anderson, and J. Daugman. Combining Cryptography with Biometrics Effectively. *IEEE Transactions on Computers*, 55(9):1081–1088, 2006.

[20] A. Juels and M. Sudan. A fuzzy vault scheme. *Proc. 2002 IEEE Int. Symp. on Information Theory*, page 408, 2002.

[21] T. C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcard-based fingerprint authentication. *Proc. ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*, pages 45–52, 2003.

[22] U. Uludag and A. K. Jain. Fuzzy fingerprint vault. *Proc. Workshop: Biometrics: Challenges Arising from Theory to Practice*, pages 13–16, 2004.

[23] K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based Fuzzy Vault: Implementation and Performance. *in IEEE Transactions on Information Forensics And Security*, 2:744–757, 2007.

[24] C. Vielhauer, R. Steinmetz, and A. Mayerhöfer. Biometric hash based on statistical features of online signatures. In *ICPR '02: Proc. of the 16 th Int. Conf. on Pattern Recognition (ICPR'02) Volume 1*, page 10123, 2002.

[25] Y. Sutcu, H. T. Sencar, and N. Memon. A secure biometric authentication scheme based on robust hashing. *MMSec '05: Proc. of the 7th Workshop on Multimedia and Security*, pages 111–116, 2005.

[26] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel. Using Voice to Generate Cryptographic Keys. *Proc. 2001: A Speaker Odyssey, The Speech Recognition Workshop*, 2001. 6 pages.

[27] A. Goh and D. C. L. Ngo. Computation of cryptographic keys from face biometrics. In *Communications and Multimedia Security (LNCS: 2828)*, pages 1–13, 2003.

[28] A. Kong, K.-H. Cheunga, D. Zhanga, M. Kamelb, and J. Youa. An analysis of BioHashing and its variants. *Pattern Recognition*, 39:1359–1368, 2006.

[29] J. Zuo, N. K. Ratha, and J. H. Connel. Cancelable iris biometric. *In Proc. of the 19th Int. Conf. on Pattern Recognition 2008 (ICPR'08)*, pages 1–4, 2008.

[30] J. Hämmerle-Uhl, E. Pschernig, , and A.Uhl. Cancelable iris biometrics using block re-mapping and image warping. *In Proc. of the Information Security Conf. 2009 (ISC'09) LNCS: 5735*, pages 135–142, 2009.

[31] M. Savvides, B.V.K.V. Kumar, and P.K. Khosla. Cancelable biometric filters for face recognition. *ICPR '04: Proc. of the Pattern Recognition, 17th Int. Conf. on (ICPR'04)*, 3:922–925, 2004.

[32] Y. Wang and K.N. Plataniotis. Face based biometric authentication with changeable and privacy preservable templates. In *Proc. of the IEEE Biometrics Symposium 2007*, pages 11–13, 2007.

[33] A. Goh, A. B. J. Teoh, and D. C. L. Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Trans. Pattern Anal. Mach. Intell.*, 28(12):1892–1901, 2006.

[34] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Optimal iris fuzzy sketches. *in Proc. 1st IEEE Int. Conf. on Biometrics: Theory, Applications, and Systems.*, pages 1–6, 2007.

[35] X. Wu, N. Qi, K. Wang, and D. Zhang. A Novel Cryptosystem based on Iris Key Generation. *Fourth Int. Conf. on Natural Computation (ICNC'08)*, pages 53–56, 2008.

[36] H. Feng and C. C. Wah. Private key generation from on-line handwritten signatures. *Information Management and Computer Security*, 10(18):159–164, 2002.

[37] A. B. J. Teoh, D. C. L. Ngo, and A. Goh. Personalised cryptographic key generation based on FaceHashing. *Computers And Security*, 2004(23):606–614, 2004.

[38] N. K. Ratha, J. H. Connell, and S. Chikkerur. Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):561–572, 2007.

[39] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri. Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *Trans. on System, Man, and Cybernetics-Part A: Systems and Humans*, 40(3):525–538, 2010.

[40] Y. Sutcu, Q. Li, and N. Memon. Secure biometric templates from fingerprint-face features. In *IEEE Conf. on Computer Vision and Pattern Recognition, CVPR '07*, pages 1–6, 2007.

[41] E. J. C. Kelkboom, X. Zhou, J. Breebaart, R. N. S. Veldhuis, and C. Busch. Multi-algorithm fusion with template protection. In *Proc. of the 3rd IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS'09)*, pages 1–7, 2009.

[42] C. Rathgeb, A. Uhl, and P. Wild. Reliability-balanced feature level fusion for fuzzy commitment scheme. In *Proc. of the Int. Joint Conf. on Biometrics (IJCB'11)*, 2011. 1–7.

[43] K. Nandakumar and A. K. Jain. Multibiometric template security using fuzzy vault. In *IEEE 2nd Int. Conf. on Biometrics: Theory, Applications, and Systems, BTAS '08*, pages 1–6, 2008.

[44] M. Y. Jeong, C. Lee, J. Kim, J. Y. Choi, K. A. Toh, and J. Kim. Changeable biometrics for appearance based face recognition. In *Proc. of Biometric Consortium Conf., 2006 Biometrics Symposium*, pages 1–5, 2006.

[45] B. Yang, C. Busch, K. de Groot, H. Xu, and R. N. J. Veldhuis. Performance evaluation of fusing protected fingerprint minutiae templates on the decision level. *Sensor-Journal, Special Issue: Hand-Based Biometrics Sensors and Systems*, 2012(12):5246–5272, 2012.

[46] K. Voderhobli, C. Pattinson, and H. Donelan. A schema for cryptographic key generation using hybrid biometrics. *7th annual postgraduate symp.: The convergence of telecommunications, networking and broadcasting, Liverpool*, 2006.

[47] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti. A multi-biometric verification system for the privacy protection of iris templates. *Proc. of the Int. Workshop on Computational Intelligence in Security for Information Systems CISIS'08*, pages 227–234, 2008.

[48] S. Kanade, D. Petrovska-Delacretaz, and B. Dorizzi. Multi-biometrics based cryptographic key regeneration scheme. In *IEEE 3rd Int. Conf. on Biometrics: Theory, Applications, and Systems, BTAS '09*, pages 1–7, 2009.

[49] V. S. Meenakshi and G. Padmavathi. Security analysis of password hardened multimodal biometric fuzzy vault. *World Academy of Science, Engineering and Technology*, 56, 2009.

[50] A. Jagadeesan, T.Thillaikkarasi, and K.Duraiswamy. Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature. *Int. Journal of Computer Applications*, 2(6):16–26, 2010.

[51] M. Zhang, B. Yang, W. Zhang, and T. Takagi. Multibiometric based secure encryption and authentication scheme with fuzzy extractor. *Int. Journal of Network Security*, 12(1):50–57, 2011.

[52] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. *EURASIP J. Adv. Signal Process*, 2008:1–17, 2008.

[53] F. Willems and T. Ignatenko. Identification and secret-key binding in binary-symmetric template-protected biometric systems. In *Proc. of IEEE Workshop on Information Forensics and Security (WIFS)*, 2010.

[54] E. J. C. Kelkboom, G. G. Molina, J. Breebaart, R. N. J. Veldhuis, T. A. M. Kevenaar, and W. Jonker. Binary biometrics: An analytic framework to estimate the performance curves under gaussian assumption. *Trans. on System, Man, and Cybernetics-Part A: Systems and Humans*, 40(3):555–571, 2010.

[55] A. Stoianov, T. Kevenaar, and M. van der Veen. Security issues of biometric encryption. In *Proc. of the Toronto Int. Conf. Science and Technology for Humanity (TIC-STH)*, pages 34–39, 2009.

[56] I. R. Buhan, J. M. Doumen, P. H. Hartel, and R. N. J. Veldhuis. Fuzzy extractors for continuous distributions. Technical report, University of Twente, 2006.

[57] E. J. C. Kelkboom, J. Breebaart, I. Buhan, and R. N. J. Veldhuis. Analytical template protection performance and maximum key size given a gaussian modeled biometric source. In *Proc. of SPIE defense, security and sensing*, 2010.

[58] T. Ignatenko and F. M. J. Willems. Information leakage in fuzzy commitment schemes. *Trans. on Information Forensics and Security*, 5(2):337–348, 2010.

[59] X. Zhou, A. Kuijper, R. N. J. Veldhuis, and C. Busch. Quantifying privacy and security of biometric fuzzy commitment. In *Int'l Joint Conf. on Biometrics - IJCB2011*, pages 1–8, 2011.