BEAT

Biometrics Evaluation and Testing

http://www.beat-eu.org/

Funded under the 7th FP (Seventh Framework Programme)

Theme SEC-2011.5.1-1
[Evaluation of identification technologies, including Biometrics]

D5.1: Privacy preservation techniques

Due date: 31/10/2012 **Submission date:** 31/10/2012
Project start date: 01/03/2012 **Duration:** 48 months
WP Manager: C. Karabat (TUBITAK) **Revision:** 1

Author(s): A. Mitrokotsa (EPFL), J. Bringer (MORPHO), C. Karabat (TUBITAK)

Project funded by the European Commission in the 7th Framework Programme (2008-2010)		
Dissemination Level		
PU	Public	No
RE	Restricted to a group specified by the consortium (includes Commission Services)	Yes
CO	Confidential, only for members of the consortium (includes Commission Services)	No

D5.1: Privacy preservation techniques

Abstract:

Biometric recognition is an important tool that offers an efficient and reliable solution to the problem of user authentication. A large number of biometric systems are used for access control applications. Without doubt the biometric technology has many favorable properties among which is included the strong link between a user and its authenticator for a biometric authentication system. Nevertheless, these advantages are also accompanied with increasing concerns about the security and privacy of biometric technology. For instance one quite serious concern for biometric systems is the fact that unlike passwords and tokens, the biometric data of a user cannot be revoked and reissued if they are compromised. In this deliverable, we investigate the privacy issues related to biometric authentication and we describe methods that can be employed in order to guarantee privacy preservation.

Contents

1 Introduction

Biometric authentication is increasingly being employed as a reliable and ultimate form of authentication and identification since it provides a strong proof of identity (i.e. a biometric something you are). However, the advantages of biometric authentication are also accompanied by some serious security risks and challenges such as accuracy, reliability, data security as well as challenges related to effective private protection. In this deliverable, we will focus mainly on the privacy issues related to biometric authentication.

Under normal conditions, when a party (i.e. a user) provides his personal identification information to a second party (i.e. the database of an authentication system), the user expects that this information will only be used for the agreed-upon function and that this information will be protected from unauthorized parties. A compromised biometric trait/template may lead to serious security and privacy threats:

(i) Biometric information may reveal very sensitive and private information such as the skin color, medical information and ethnic origin and thus, may further lead to unjustified discriminations.

(ii) It is easy to realize the privacy implications if we consider that unique identifiers and biometric data may be easily collected without knowledge or consent.

(iii) Biometric traits that are cross-matched and used in different biometric databases raise serious issues regarding the linkability that may further lead to tracking and profiling and surveillance of individuals.

(iv) This risk is even more serious if we consider that biometric data unlike passwords or other ways of authentication and identification cannot be revoked (inherent irrevocability) and the compromise of a biometric trait-database leads to serious threats of identity (data breach, identity theft and fraud).

Some of the most important questions that we need to ask in order to investigate risks and threats regarding privacy invasiveness in each application scenario are the following:

- Is the used system optional or mandatory?
- Is the system used for identification or verification?
- Is the system deployed for a fixed period of time?
- Who owns the biometric information?
- Where is the biometric data stored?
- What type of biometric technology is being deployed?
- Does the system use biometric templates, biometric images or both?

The International ISO/IEC 24745 standard [1] “Information technology - Security techniques - Biometric information protection” provides guidelines that should be followed in order to protect biometric data/information and guarantee their confidentiality, integrity and revocability while this information is stored and transfered.

More precisely, the ISO/IEC 24745 standard provides:

- A description of the inherent threats to which biometric systems are exposed as well as the countermeasures that can be employed in order to protect them.

- The security requirements that are necessary in order to guarantee the secure binding between a biometric template/trait and a user. More precisely, the need for irreversibility, unlinkability and confidentiality. A detailed description of these requirements that constitute also criteria-metrics for benchmarking privacy-preserving biometrics is provided in Section 4.
- As well as guidelines that maybe followed in order to guarantee the privacy of the involved parties while the biometric information is stored, transfered and processed.

Privacy-preservation in biometric authentication has also been investigated by other European research projects. For instance the project TrUsted Revocable Biometric IdeNtitiEs (TURBINE) (http://www.turbine-project.org) is investigating the protection of fingerprint templates. Additionally, the TURBINE project has received an opinion [31] from the EDPS (European Data Protection Supervisor) in which is acknowledged the relevance of the best practices provided as output of this project. Furthermore, the BEST (Biometrics European Stake-holders) Network tries to investigate how biometrics can most appropriately be applied in the context of the Charter of Fundamental Rights of the European Union.

This deliverable is organised as following: in section 2 we describe biometric privacy-preservation techniques that can be employed in order to guarantee no violation of the privacy rights of the involved parties. In section 3 we describe attacks that can be mounted against privacy preservation techniques. Section 4 describe the criteria-metrics that can be used to benchmark template protection algorithms while section 5 concludes this deliverable.

2 Related work: Privacy-preserving techniques

Privacy-preserving techniques can be discriminated into two broad categories: *hardware-based* approaches and *software-based* approaches.

Hardware-based approaches: A *hardware-based* approach involves designing a "closed" recognition system. In such a system the biometric template never leaves a physically secure module such as a *smart card* or a *hand-held device.* Such a device matches the input biometric trait with the template stored in the device and releases a key in case the authentication is successful.

Software-based approaches: Software-based approaches protect the biometric template by storing a modified version of it, in order to reveal as little as possible information about the original biometric trait. Software-based approaches can be discriminated into two main categories: *template or feature transformation* and *biometric cryptosystems:*

- *Template or Feature Transformation* transform the biometric template based on parameters derived from external information such as user passwords or keys. The same transformation function is applied to the query and matched with the stored template.

- *Biometric Cryptosystems* attempt to obtain error correcting information from the biometric features known as helper or auxiliary data. The later does not reveal significant information about the biometric trait or the key. Furthermore, error correcting codes are employed in order to recover the enrolled biometric features or the employed key.

- *Combined template transformation* and *biometric cryptosystems:* Some approaches combine template transformation and biometric cryptosystems in order to achieve privacy-preservation. For instance Nandakumar *et al.* [69] use the transformed template as input to a biometric cryptosystem while Bringer *et al.* [8] transform the helper data in a biometric cryptosystem using an homomorphic scheme.

2.1 Template or Feature Transformation

One of the main advantages of template or feature transformation techniques is firstly that the generated templates through this transformation approach can be easily revoked (for instance by changing the password or the key used). Furthermore, there are fewer restrictions regarding the matching algorithms. Thus, it is possible to design sophisticated matchers that can robustly handle intra-user variations. On the other hand, one of their main disadvantages is the difficulty to measure their security strength. An interesting security analysis of template transformation techniques have been described by Nagar *et al.* [66].

Template or feature transformation techniques can be discriminated into two main categories based on the template representation used: *vector-based* transformation and *interest-point based* transformation.

Vector based transformation: In *vector-based transformation* biometric templates are represented as vectors and the dissimilarity between two vectors is computed based on the Hamming distance. One of the main requirements of vector-based transformation techniques is the fact that the distances between the vectors should be preserved before and after the transformation. Below we list some of the most important vector-based transformation techniques:

- *Cancelable biometric data*: Ratha *et al.* [73] introduced the concept of transforming a biometric image in order to enhance the privacy of these biometric data. When non-invertible, this transformation may prevent an adversary to find back who this transformed image belongs to. Moreover it is easy to renew the stored template by choosing a different transformation or to have different transformations for different applications. The question of the irreversibility of the transformation is raised in [3] and information on the accuracy performance of the matching are given in [71, 72]. One difficult constraint of this scheme is the tradeoff between performances drop and irreversibility: the transformation has to decrease the entropy of the biometric data to be truly irreversible; therefore this has a bad impact on the performances.

Nevertheless the idea of transforming the image or the template seems to be helpful to enhance the security when applying other protection schemes (like in [15]). The capability to renew the transformation function is exploited in [16] to design a one-time biometric identification scheme similarly to the well known one-time password principle.

- *Biometric hashing or Biohashing:* Biohashing [85, 40] is an emerging privacy-preserving technique which represents a biometric feature vector as a pseudo-random binary sequence by incorporating it with random number generator [60, 85, 40, 46, 47, 44, 48, 45]. It is completely different than cryptographic hashing. Biohashing techniques use the biometric template and a secret key (via token) in order to generate the biohash vector of a user. In other words, these techniques rely on two-factor authentication. Since a user cannot give exactly the same biometric data to the system at each attempt to enter the system, it is expected that the distance between the biohash vectors of the same user are small and the distance between the biohash vectors of the different users are high. On the other hand, one bit change at the input, results to huge changes at the output in cryptographic hashing techniques. Thus, they are not suitable to use in biometric recognition systems. Biohashing techniques generally use random projection for dimension reduction just after a feature extraction method (i.e. Principle Component Analysis (PCA), Linear Discriminant Analysis (LDA), Discrete Wavelet Transform (DWT), Fourier Mellin Transform etc.). Furthermore, they use binary quantization to obtain a binary vector which is called biohash. Biohashing techniques achieve very high recognition rates under normal conditions. If the secret key is obtained by an attacker, their performance decreases dramatically [61, 53]. Quantization of biometric feature vector and dimension reduction may also affect directly the performance of a biohashing technique [46, 47]. Apart from that, these methods suffer from invertibility attacks [52, 25]. In these attacks, it is assumed that an adversary gets the biohash and its associated secret key and she tries to obtain the biometric template of the user.

  Biohashing techniques are applied to various biometrics. For face biometrics generally PCA or LDA are used as a feature extraction method before applying a random projection [60, 85, 46, 47]. Teoh *et al.* [40] proposed a biohashing technique for fingerprint biometrics. This method uses integrated wavelet and Fourier Mellin transform for feature extraction and random projections for dimension reduction. The PalmHash [27] technique, which uses LDA and random dimension reduction methods, is proposed for palm biometrics.

  Advantages of Biohashing Techniques: The main advantages of *biohashing* are: (i) their suitability for match-on-card application, (ii) the fact that they provide fast authentication due to linear operations and the fact that comparisons are performed in the binary domain, (iii) they provide high recognition rates under ideal conditions.

  Disadvantages of Biohashing Techniques: The main disadvantage of the biohashing approach is the poor recognition performance in case that an attacker gets the secret key. Additionally, invertibility problems may be generated due to linear operations (for instance the biometric template may be obtained if the biohash and its secret key are obtained).

- *BioPhasor* [41, 41]: BioPhasor techniques are proposed to improve the biohashing techniques. In these methods, the rows of the orthogonal transformation matrix are used as the imaginary part and added to the biometric vector to obtain a set of complex vectors. For each of these vectors, the argument of the values in them are averaged and quantized to form the final binary template. This transformation has been shown to better preserve the matching performance even if the secret key is known to the adversary. Although this scheme is claimed to be non-invertible, the complexity involved in inverting this transformation is not known.

  The main advantage of the BioPhasor techniques is that it is computationally hard to invert the resulting vector in order to obtain the original biometric trait. While the main disadvantage of the BioPhasor techniques is the high complexity in order to perform the required computations and consequently the increased required time for authentication time.

- *Robust Hashing*: *Robust hashing* [84] techniques use a non-invertible transformation function which is a one-way function. The aim is to make the biometric template secure.

  Advantages of Robust Hashing Techniques: The main advantages of *robust hashing* techniques are: (i) It is computationally hard to invert robust hash vector in order to obtain biometric data, (ii) They are quite secure since they use nonlinear operations.

  Disadvantages of Robust Hashing Techniques: Among the main disadvantages of robust hashing techniques are included: (i) They use complex dimension reduction methods, (ii) They require high authentication time in comparison with biohashing techniques due to nonlinear operations, (iii) There is a trade-off between discriminability and non-invertibility.

- *Class Distribution Preserving Transformation*: These techniques transform a real-value biometric template to a binary string by taking into account the geometric relationship between the biometric templates. Feng *et al.* [34] proposed a method where the biometric template is transformed into a binary string by randomly selecting a set of vectors of the same dimension as the biometric template. Then, the Euclidean distances of the biometric vector from these vectors are stored. Therefore, the aim is to preserve the class distribution when binarizing the biometric templates. These techniques incorporate error correction methods (i.e. BCH coding) and traditional cryptographic hashing methods in order to guarantee the non-invertibility [34]. Besides, Karabat *et al.* [48] proposed a method which uses an optimal linear transformation matrix based on within-class covariance matrix which is the maximum likelihood estimate of the variations of the biometric data belonging to the same user. This method also aims to reduce the error by taking into account within class distributions. However, it does not use any error correction coding methods.

Advantages of Class Distribution Preserving Transformation: Among the main advantages of class distribution preserving transformation techniques are included: (i) They provide provable security due to cryptographic hashing methods. (ii) They require high complexity in order to invert the template.

Disadvantages of Class Distribution Preserving Transformation: Among the main disadvantages of class distribution preserving transformation are included: (i) Requirement for high computation resources at the enrollment stage. (ii) It incorporates error correction methods and thus requests more computation resources at the enrollment and authentication stages.

Interest point based transformation: Fingerprint biometric templates are usually represented by a set of points called minutiae. Thus, transformation-based approaches used for fingerprint biometrics should use minutiae as the initial representation while the final representation in the transformed domain should also be in the form of a minutiae.

Ratha *et al.* [71] have proposed an approach called cancelable fingerprint templates that uses three different minutiae transformation techniques: the cartesian, polar and functional transformation. All these transformations proposed by Ratha *et al.* [71] have as main advantage the fact that it is difficult to invert them. Nevertheless, these transformations lead to increased intra-user variations (i.e. changes in the template of the same user) and thus consequently to an increased false rejection rate. We should note here that there are many techniques specific for minutiae representation of fingerprints but they use similar techniques compared to vector-based transformation (i.e. cancelable transformation or secret-based transformation).

2.2 Biometric Cryptosystems

Other terms used for biometric cryptosystems are: *biometric encryption*, *fuzzy extractor*, *secure sketch*, *helper data system*, *biometric locking*, *biometric key generation.*

Biometric encryption can de defined as the process in which a digital key (randomly generated) is bound to a biometric template (*key binding*) or a key is generated by a biometric template (i.e. *key generation*). In both modes ("*key binding*" and "*key generation*") of the biometric encryption (BE) methods, the key is "encrypted" with the biometric trait and the result, which is usually called *biometrically encrypted key* or *BE template* or *helper data* is stored either in a database or locally (i.e. smart card).

The BE template can be "decrypted" in the verification process only if the correct biometric sample is presented. Since at each verification process a fresh biometric trait/sample is presented this biometric "encryption/decryption" process is fuzzy by nature. Thus, one important challenge is to recreate the same digital key despite the variations in the biometric traits.

Some BE approaches (for instance the *Fuzzy Vault* [42] and *Fuzzy Commitment* schemes [43, 36]) work equally well with both *key binding* and *key generation* mode.

The *key generation* mode is also called *secure sketch* or *fuzzy extractor*. In this case the original (enrolled) biometric template is recovered in the verification process when a fresh biometric sample is applied to the BE template. In this mode the enrolled biometric template or a string derived from it for instance its hash value serves as a digital key. Nevertheless, this key changes upon each enrollment.

In the *key binding* mode the key is randomly generated. Thus, the user does not know the key and it can be easily changed since it does not depend on the biometric trait.

Advantages of biometric cryptosystems: The main advantages of biometric cryptosystems include: (i) Firstly, we can easily understand and evaluate the security strength in information-theoretic terms. (ii) Additionally, with biometric systems the key is bound with the biometric trait and thus privacy and security is enhanced. (iii) Using a biometric cryptosystem a biometric system is less susceptible to high level security attacks. (iv) Furthermore, by employing a biometric cryptosystem, the biometric image or any other conventional biometric template is not stored. (v) It is computationally difficult to recreate the original biometric image/template from the stored information. (vi) A large number of untraceable templates for the same biometric can be created for different applications. (vii) Untraceable templates from different applications cannot be linked. (viii) Untraceable templates can be renewed or revoked. (ix) In these systems keys are longer than conventional passwords and they do not require user memorisation.

Disadvantages of Biometric Cryptosystems: Among the main disadvantages of biometric cryptosystems are included: (i) The fact that we cannot use any sophisticated matchers. (ii) The matching performance of a biometric cryptosystem is limited by the error-correction capability of the code used. (iii) To improve the performance we need to extract invariant and discriminative features from the biometric trait.

Below we list some of the most important privacy-preservation techniques for biometrics based on biometric cryptosystems:

- *Secure Sketch:* It has been suggested [43, 29] to replace the traditional algorithms to compare biometric traits by an error correction procedure by means of Secure Sketch. In fact, in a secure sketch, biometric data are quantized and then combined with a codeword to exploit its correction capacity. In this case, the biometric template – the secure sketch – partially hides the biometric reference which was used in its creation. However, secure sketch suffers from two drawbacks. The first one is that the error correction is, usually, less effective than the traditional matching algorithm to compare two biometric traits regarding the accuracy of the performances. The second one is that secure sketch is not sufficient to ensure the confidentiality of the underlying biometric trait used alone [10, 76]. A potential benefit of the secure sketch is the simplification of the biometric matching. This opens the possibility to encrypt the secure sketch with a homomorphic cryptosystem to perform the comparison with encrypted biometric data, i.e. without decrypting them. Consequently, there have been a lot of papers integrating secure sketches into cryptographic protocols to reinforce their security [17, 13, 4, 8, 83, 32, 70].

- *Fuzzy Vault:* The fuzzy vault has been introduced by [42] and many papers describe applications of this scheme to fingerprint, e.g. [26, 55, 64, 59, 23, 58, 56, 57, 65, 69, 68, 88]. This scheme, that belong in the category of secure-sketch schemes, relies on Reed-Solomon codes: each information symbol is accompanied by its evaluation by a given polynomial p to form a pair $(x_i, y_i = p(x_i))$. Moreover, some random chaff points are added to mix genuine pairs with fake ones. As this construction is order-invariant, it can be applied to fingerprint biometric where minutiae play the role of the x_i's. To open a vault, one has to produce a sufficient number of genuine pairs; this way, the errors decoding capacity of the Reed-Solomon code enables to reconstruct the underlying polynomial p. The feasibility of using such concept to identification is now studied [63] and an extension for encoding multiple sets has recently been suggested [12].

- *Mytec1:* Mytec1 is the first biometric encryption (BE) scheme based on key binding and was proposed by Soutar *et al.* [81]. In this approach the key is linked to a predefined pattern s From s and f and their Fourrier transforms S and F correspondingly a filter is created $H = S/F$ [22]. Only the value of H is stored and obtaining S or F is quite difficult. If for another fingerprint f' with corresponding Fourrier trasfer F' it holds that $F = F'$ then the verification process outputs s' such that $s = s'$. Nevertheless, this approach turned out to be impractical regarding the provided accuracy and security.

- *Mytec2:* Mytec2 [80, 78, 79] was a successor of Mytec1 and it was the first practical biometric encryption scheme. In this approach only the phase-parts of the Fourier tansforms S and F are held in the filter H. Furthermore, the phase of S is randomly generated and not stored. Consequently, the output of this approach c is also random. The output pattern and the key are linked via a lookup table and ECC while the key, the filter H, the hashed key and lookup table are stored in the helper data. The main advantage of this approach is error tolerance. Nevertheless, the initial published version was vulnerable to hill-climbing attacks (see Section) since it uses a simple repetition ECC. For more proper selections of ECC the security of the approach is increased.

- *Fuzzy Commitment Schemes:* The Fuzzy Commitment [43, 36, 9, 89, 86] belongs in the category of secure-sketch schemes and is probably the simplest BE approach and most studied one. In this approach the biometric template should be in the form of an ordered bit string with a fixed length. A key is mapped to an (n, k, d) ECC codeword that has the same length with the biometric template. The codeword and the template are XOR-ed and the resulting value as well as a hashed value of the key are stored. Upon the versification process a fresh biometric template is XOR-ed with the stored string and the resuling value is decoded using the ECC scheme. If the codeword received from this process agrees with the enrolled (original) biometric template the k-bit key is released.

2.3 Dedicated Encoded Techniques

A lot of suggestions have been published to apply the above described constructions to classical biometric data. One common problem that arises for most of the schemes - in particular for *biometric cryptosystems* - is the need for dedicated encoding of biometric data to get good accuracy performances. Often, it is needed to find a binarisation process (see for instance [49]) of biometric data that enables to compare them with a simple algorithm as for instance Hamming distance, while it is required to maintain the discriminative properties of the data.

The case of iris is generally considered as one the simplest ones: Iriscodes [28] are a common way of representing iris trait as binary vectors. To represent iris, biometric data are quantized (binarised) in such a way that for comparing two iriscodes one has to look at the number of coordinates in which they differ. However, the score computation relies also on a more or less complex normalization process that takes into account the quantity of information available after the feature extraction from the iris images. This as an impact on the way to design the protected comparison algorithm [10].

Face templates are commonly represented in an Euclidean space. Hence it is possible to use state-of-the-art embedding techniques into a Hamming space for binarisation. However the constraints on performances could be hard to fulfill as seen in the literature [87, 51].

Fingerprint case is a tricky one and thus is the subject of a lot of scientific works [86, 39, 24, 15, 30, 67, 90, 33, 91]. One natural solution to binarize a fingerprint is to start from the image, to extract the global pattern (mainly ridges orientation) of the fingerprint and then to adapt state-of-the-art quantization techniques. However, this is not based on classical fingerprint templates [37] that use minutiae and for which performances are known to be far better than with the fingerprint pattern and most of the methods need a reliable alignment of the data. Gyaourova and Ross [35] solution is also based on pattern but exploits the comparison with representative fingerprint patterns to construct a feature vector. Several works suggest solutions at minutiae level, for instance [30, 67, 90, 33]. And some recent proposals, e.g. [91], are more precisely based on local neighborhoods of a minutia – called minutiae vicinities. In particular [19, 20, 21] offers promising performances with binary feature vectors that can be compared two by two with a matching phase that exploits the Hamming distance and some additional localization information.

Similar solutions would be necessary for the other biometric modalities. And in all cases, improvement of the performances (i.e. decrease of the impact of the binarisation algorithms onto the error rates) is still an important research topic.

2.4 Other approaches

HW-based: A technology known as Match-On-Card (MOC) enables to realize the comparison of the fresh biometric trait to a biometric template stored inside a smartcard by processing the complete matching algorithm during a biometric authentication request. As a next step the smart card gives as output whether this comparison is positive or not.

In [18], this is exploited to combine local authentication on a local client, based on a traditional biometric comparison. After this local authentication, a specific anonymous remote authentication – relying on a cryptographic key generated from the stored biometric template – is executed where the server can only verify the validity of the individual without learning its identity. In [14], the technology is used to embed a security module in local access control terminal to ensure the protection of the reference data: the protocol enables to achieve authorization checking. These systems have been analyzed and demonstrated within the TURBINE project, see `http://www.turbine-project.eu/index.php`.

In the case of MOC-enabled smart cards, it is important to prevent vulnerabilities similar to these of a YesCard (i.e. an attack that has been performed in banking systems, where a card always returns "yes"). In the case of biometric systems this attack can lead not only to the *YesCard* even but also to the *NoCard* as it is described by Barral *et al.* [6]. More precisely, Barral and Vaudenay [6] proposed a protocol that can be used in order to combat attacks that my lead to YesCard or NoCard events using simple cryptographic primitives such as symmetric encryption. Barral *et al.* have also proposed an approach called *externalised fingerprint matching* [5]. In this approach a smart card is employed for the biometric identification. In order to perform the identification the following protocol is used. A scrambled fingerprint template t, derived from the original template by adding a random minutiae at the enrollment phase, is stored on the smartcard. Additionally, on the card is stored a string w in which is encoded, which of the minutiae in t are genuine. In the identification process, the terminal reads t from the card and using the incoming data (fresh biometric trait), it determines which of the minutiae in t are genuine. More precisely, the terminal used in the identification process generates a candidate w' and sends this to the card. As a final step the card checks if the Hamming weight of $w \oplus w'$ is smaller than a security threshold d.

3 Attacks and Security analysis

Simoens *et al.* [76] present attacks on template protection schemes that can be described as fuzzy sketches based on error-correcting codes. A number of attacks against biometric cryptosystems (biometric encryption) approaches are presented in [82]. Below, we give a brief description for some of the most representative attacks against privacy-preserving biometric systems.

- *False acceptance rate (FAR) attacks:* As explained since several years [54, 11] in the case of the fuzzy commitment scheme, one very concrete vulnerability of protection schemes that work at the template level only, is the capability to execute authentication checks with any restriction based on chosen or random fresh templates. In practice, an adversary that possesses a large database of biometric templates and that has access to a so-called protected template will be able to run a search among the database until he finds a False Accept (i.e. a template sufficiently close to the protected one). This way he will be able to retrieve data close to the original one, and sometimes this would even lead directly to the original template (this is the case for the fuzzy commitment scheme). It should be noted here that the False Accept Rate (FAR) is in general between 10^{-5} and 10^{-3} which is sufficiently low to achieve a strong authentication but not negligible at all. Hence this represents an important threat.

- *Cross-matching attacks:* Simoens *et al.* [76] explains how to determine whether two secure sketches are coming from the same biometric source in the case of the fuzzy commitment scheme. This attack may also lead to the reconstruction of the template under some constraints. Indistinguishability is highlighted there as a specific property to be addressed by protection schemes. Later on, Kelkboom *et al.*[50] suggested to use a permutation of the templates as a potential countermeasure against such cross-matching checks between different sketches.

- *Inverting hash:* This is a type of brute force attack. In case that a hash is stored on the BE template (i.e. helper data) an attacker may try to cryptographically invert the hash. In order to avoid this type of attack, it should always be computationally infeasible for the attacker to mount such an attack.

- *Hill-climbing attack* : In a *hill-climbing* attack [2, 62] the adversary sends random synthetically generated templates to a biometric authentication system (matcher) which are modified one after the other (iteratitely). More precisely, the attacker makes small modifications in the input impostor's image and waits to see how the acceptance scores (intermediate matching scores since the BE algorithm does not provide scores) change. In case that the acceptance score increases, then the modification of the input impostor's image is retained otherwise the adversary tries a different modification. After multiple repetitions of this process the attacker will be able to reach the verification threshold (δ).

- *Nearest Impostors attack:* In the *nearest impostor* attack, similarly to the *hill-climbing* attack the adversary uses a partial matching score of the ECC chuck of the BE template and a global intermediate score. Nevertheless, instead of using the same image and making multiple modifications on it the attacker uses a relatively small (for instance a few hundreds) number of samples against the BE template. Thus, he identifies multiple nearest impostors (i.e. synthetically generated templates) and keeps those for which he achieves either the highest global score or the higher partial score for a given chunk. He applies this technique iteratively and by using a voting technique, he retrieves the key bits related to each chunck. If the attacker succeeds he will be able to recover the whole key or at least reduce the key space.

- *ECC Histogram attack* [82]: In some BE approaches, ECC is used in order to generate the BE template (i.e. helper data). In some cases the ECC codeword is composed of a series of chunks (i.e. for instance the Reed-Muller chunks [36]). An adversary may exploit this by generating a database of artificially generated templates and run it against the ECC chunks of the helper data. By counting the number of appearances of each possible output codeword for all artificially generated templates in his database, he creates a histogram. Finally, he selects the codeword that corresponds to the histogram winner.

- *Re-usability attack* [7], [74]: In case that the same biometric is used in multiple applications, an adversary may try to use several versions of the helper data in order to retrieve the original biometric trait and /or the key. The *Fuzzy Vault* approach is especially vulnerable against this type of attack.

- *Blended Substitution attack* [74]: In a *blended substitution* attack, the adversary substitutes the user's biometric record with his own data. This way both the user and the adversary are able to be authenticated with the same enrolled biometric record. The fuzzy vault scheme is especially vulnerable to this attack. In such a scheme, the adversary may insert his own biometric template using his own key or using the user's key if he has it in his disposal. In the later case, the attack is called *insidious blending.*

- *Non-randomness attacks* [82]: In this category are included all the attacks that can be launched against biometric systems by exploiting the non-randomness of biometric helper data. More precisely, many Biometric Encryption schemes such as the Fuzzy Vault and the Fuzzy Commitment schemes assume that the biometric traits are random in order to formally prove their security. Nevertheless, in reality the biometric traits are inherently non-random. Thus, an adversary may exploit this to identify clusters in the helper data and subsequently interconnect the same parity bits.

Frameworks to analyse the privacy of biometric approaches: In [75], a general framework is introduced to analyze the privacy properties of biometric authentication protocols. The goal of an adversary in such context is to learn information either on biometric data or on users that are in the system, not to bypass the authentication. A general model involving four logical entities – sensor, server, database and matcher – is described and complex internal adversaries are studied. This work underlines that current solutions that have been developed in the honest-but-curious adversary model, would probably have weaknesses when considered in an insider attack model. This emphasizes the need to go beyond the usual honest-but-curious assumption.

4 Criteria-metrics for Benchmarking Privacy-preserving Biometrics

A detailed description of criteria-metrics that could be used to benchmark template protection algorithms is given in [77, 38]. Below we briefly describe the most important metrics that should be taken into consideration when designing privacy-preserving biometric systems.

- *Accuracy:* The biometric template protection scheme should not degrade the recognition performance (i.e. the False Acceptance Rate (FAR) and the False Rejection Rate (FRR)) of the biometric system.
- *Diversity:* The biometric template should not allow cross-matching across the existing databases. In other words, the biometric template protection scheme should allow the generation of a maximum number of independent protected templates that can be generated from the same biometric feature.
- *Irreversibility:* It is of utmost importance that it is computationally infeasible to retrieve the original biometric template from the protected (or transformed one). Due to this requirement the transformation approach that might be adopted may lead to lower accuracy rate (difficult to achieve high accuracy).
- *Revocability:* It should be possible and straightforward to revoke a compromised template and generate a new one for the same user.
- *Security:* It should be computationally infeasible to obtain the original biometric template from the secure-transformed biometric template. Thus, it would be computationally infeasible for an adversary to generate a physical spoof of the biometric trait from a stolen template.
- *Unlinkability:* It is important to protect the users of a biometric system from cross-matching of different biometric trait databases. This way the users of a biometric trait are protected from possible tracing and profiling.

5 Conclusions

Obviously privacy-preservation is an important requirement of utmost importance in order to guarantee the widespread adoption of biometric authentication systems. Nevertheless, this direct need for privacy-preserving biometric systems is often accompanied by a “zero-sum” mentality that considers that the adoption of privacy-preserving techniques in the authentication information systems will necessarily weaken the security and functionality of these systems. In this deliverable, we discuss existing privacy-preservation techniques designed for biometric systems. It is quite important to note that guaranteeing that no privacy-rights are violated during the biometric authentication process has received a lot of attention. Many privacy-preserving constructions for biometric systems have been proposed while the attack and security analysis studies are increasing. Undoubtedly, several security properties/constraints should be taken under consideration when designing a privacy-preserving mechanism for a biometric system and many of the existing schemes present serious limitations. For instance, the security of template level techniques is inherently limited by the False Acceptance Rate [54]. However, given the increased interest and motivation toward this direction we expect to see important progress in this field that would lead to a "win-win" scenario for all the entities involved without violating their privacy rights.

References

[1] S. I. 24745:2011. Information technology – security techniques – biometric information protection.

[2] A. Adler. Vulnerabilities in biometric encryption systems. In *Proceedings of the International Conference on Audio and Video based Biometric Person Authentication*, pages 1100–1109, 2005.

[3] R. Ang, R. Safavi-Naini, and L. McAven. Cancelable key-based fingerprint templates. In *ACISP*, pages 242–252, 2005.

[4] M. Barbosa, T. Brouard, S. Cauchie, and S. M. de Sousa. Secure biometric authentication with improved accuracy. In *ACISP*, pages 21–36, 2008.

[5] C. Barral, J.-S. Coron, and D. Naccache. Externalized fingerprint matching. In *Biometric Authentication*, volume 3072 of *LNCS*, pages 309–315, 2004.

[6] C. Barral and S. Vaudenay. A Protection Scheme for MoC-Enabled Smart Cards. In *Proceedings of the Biometric Symposium BSYM'06*, pages 1–6. IEEE, 2006.

[7] X. Boyen. Reusable cryptographic fuzzy extractors. In *ACM CCS 2004, ACM*, pages 82–91. ACM Press, 2004.

[8] J. Bringer and H. Chabanne. An authentication protocol with encrypted biometric data. In *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology*, AFRICACRYPT'08, pages 109–124, Berlin, Heidelberg, 2008. Springer-Verlag.

[9] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Optimal iris fuzzy sketches. In *Proceedings of the 1st IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS 2007)*, Sept 2007.

[10] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Theoretical and practical boundaries of binary secure sketches. *IEEE Transactions on Information Forensics and Security*, 3(4):673–683, December 2008.

[11] J. Bringer, H. Chabanne, and Q. D. Do. A fuzzy sketch with trapdoor. *IEEE Transactions on Information Theory*, 52(5):2266–2269, 2006.

[12] J. Bringer, H. Chabanne, and M. Favre. Fuzzy vault for multiple users. In *AFRICACRYPT*, pages 67–81, 2012.

[13] J. Bringer, H. Chabanne, M. Izabachène, D. Pointcheval, Q. Tang, and S. Zimmer. An Application of the Goldwasser-Micali Cryptosystem to Biometric Authentication. In *ACISP*, pages 96–106, 2007.

[14] J. Bringer, H. Chabanne, T. A. M. Kevenaar, and B. Kindarji. Extending match-on-card to local biometric identification. In *Biometric ID Management and Multimodal Communication, BioID-Multicomm 2009*, volume 5707 of *LNCS*, 2009.

[15] J. Bringer, H. Chabanne, and B. Kindarji. The best of both worlds: Applying secure sketches to cancelable biometrics. *Science of Computer Programming*, 74(1-2):43–51, 2008. Special Issue on Security and Trust.

[16] J. Bringer, H. Chabanne, and B. Kindarji. Anonymous identification with cancelable biometrics. In *International Symposium on Image and Signal Processing and Analysis, ISPA*, 2009.

[17] J. Bringer, H. Chabanne, D. Pointcheval, and Q. Tang. Extended private information retrieval and its application in biometrics authentications. In *CANS*, pages 175–193, 2007.

[18] J. Bringer, H. Chabanne, D. Pointcheval, and S. Zimmer. An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication. In *IWSEC*, 2008.

[19] J. Bringer and V. Despiegel. Binary feature vector fingerprint representation from minutiae vicinities. In *Biometrics: Theory, Applications, and Systems, 2010. BTAS'10. IEEE 4th International Conference on*, 2010.

[20] J. Bringer, V. Despiegel, and M. Favre. Adding localization information in a fingerprint binary feature vector representation. In *SPIE Defense, Security and Sensing, Biometric Technology for Human Identification*, 2011.

[21] R. Cappelli, M. Ferrara, and D. Maltoni. Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 99(PrePrints), 2010.

[22] A. Cavoukian and A. Stoianov. Biometric encryption. In *Encyclopedia of Biometrics*, LLC. Springer Science and Business Media, 2009.

[23] S.-H. Chae, S. J. Lim, S.-H. Bae, Y. Chung, and S. B. Pan. Parallel processing of the fuzzy fingerprint vault based on geometric hashing. *TIIS*, 4(6):1294–1310, 2010.

[24] C. Chen and R. N. J. Veldhuis. Binary biometric representation through pairwise polar quantization. In *ICB*, pages 72–81, 2009.

[25] K. H. Cheung, A. W.-K. Kong, J. You, and D. Zhang. An analysis on invertibility of cancelable biometrics based on biohashing. In *CISST*, pages 40–45, 2005.

[26] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn. Automatic alignment of fingerprint features for fuzzy fingerprint vault. In *CISC*, pages 358–369, 2005.

[27] T. Connie, A. Teoh, M. Goh, and D. Ngo. Palmhashing: a novel approach for cancelable biometrics. *Inf. Process. Lett.*, 93(1):1–5, Jan. 2005.

[28] J. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. Pattern Anal. Mach. Intell.*, 15(11):1148–1161, 1993.

[29] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *EUROCRYPT*, pages 523–540, 2004.

[30] S. Draper, J. Yedidia, S. C. Draper, A. Khisti, A. Khisti, E. Martinian, E. Martinian, A. Vetro, A. Vetro, and J. S. Yedidia. Using distributed source coding to secure fingerprint biometrics. In *in Int. Conf. Acoutics Speech Signal Proc*, pages 129–132, 2007.

[31] EDPS. Opinion 1.02.2011 on a research project funded by the european union under the 7th framework programme (fp7) for research and technology development (turbine (trusted revocable biometric identities), 14 p.

[32] P. Failla, Y. Sutcu, and M. Barni. eSketch: a Privacy-Preserving Fuzzy Commitment Scheme for Authentication using Encrypted Biometrics . In *ACM MMSec'10*, 2010.

[33] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. K. Ratha. Anonymous and revocable fingerprint recognition. In *CVPR*, 2007.

[34] Y. C. Feng and P. C. Yuen. Selection of distinguish points for class distribution preserving transform for biometric template protection. In *ICB*, pages 636–645, 2007.

[35] A. Gyaourova and A. Ross. A novel coding scheme for indexing fingerprint patterns. In *SSPR/SPR*, pages 755–764, 2008.

[36] F. Hao, R. Anderson, and J. Daugman. Combining crypto with biometric effectively. *IEEE Transactions On Computers*, 55(9):1081–1088, 2006.

[37] ISO/IEC 19794-2:2005. Information technology, biometric data interchange formats, part 2: Finger minutiae data. Technical report, ISO/IEC, 2005.

[38] A. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal Advances Signal Proceedings*, pages 1–17, 2008.

[39] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti. Fingercode: A filterbank for fingerprint representation and matching. In *CVPR*, pages 2187–, 1999.

[40] A. T. B. Jin, D. N. C. Ling, and A. Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*, 37(11):2245–2255, 2004.

[41] A. T. B. Jin, K.-A. Toh, and Y. W. Kuan. 2Ns Discretisation of BioPhasor in Cancellable Biometrics. In S.-W. Lee and S. Z. Li, editors, *ICB*, volume 4642 of *Lecture Notes in Computer Science*, pages 435–444. Springer, 2007.

[42] A. Juels and M. Sudan. A fuzzy vault scheme. *Des. Codes Cryptography*, 38(2):237–257, Feb. 2006.

[43] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security*, CCS '99, pages 28–36, New York, NY, USA, 1999. ACM.

[44] C. Karabat and H. Erdogan. A cancelable biometric hashing for secure biometric verification system. In *Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pages 1082–1085, 2009.

[45] C. Karabat and H. Erdogan. Trustworthy biometric hashing method. In *Signal Processing and Communications Applications Conference, 2009. SIU 2009. IEEE 17th*, pages 65 –68, april 2009.

[46] C. Karabat and H. Erdogan. Discriminative projection selection based face image hashing. *IEICE Transactions*, 95-D(5):1547–1551, 2012.

[47] C. Karabat and H. Erdogan. Error-correcting output codes guided quantization for biometric hashing. *IEICE Transactions*, 95-D(6):1707–1712, 2012.

[48] C. Karabat, H. Erdogan, and M. Mihcak. A face image hashing method based on optimal linear transform under colored gaussian noise assumption. In *Digital Signal Processing (DSP), 2011 17th International Conference on*, pages 1 –6, july 2011.

[49] E. Kelkboom, G. Molina, T. Kevenaar, R. Veldhuis, and W. Jonker. Binary biometrics: An analytic framework to estimate the bit error probability under gaussian assumption. In *IEEE BTAS 2008*, pages 1–6, 2008.

[50] E. J. C. Kelkboom, J. Breebaart, T. A. M. Kevenaar, I. Buhan, and R. N. J. Veldhuis. Preventing the decodability attack based cross-matching in a fuzzy commitment scheme. *IEEE Transactions on Information Forensics and Security*, 6(1):107–121, 2011.

[51] T. A. M. Kevenaar, G. J. Schrijen, M. van der Veen, A. H. M. Akkermans, and F. Zuo. Face recognition with renewable and privacy preserving binary templates. In *AUTOID '05: Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies*, pages 21–26, Washington, DC, USA, 2005. IEEE Computer Society.

[52] K. Kommel and C. Vielhauer. Reverse-engineer methods on a biometric hash algorithm for dynamic handwriting. In *Proceedings of the 12th ACM workshop on Multimedia and security*, MM&#38;Sec '10, pages 67–72, 2010.

[53] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You. An analysis of biohashing and its variants. *Pattern Recogn.*, 39:1359–1368, July 2006.

[54] U. Korte and R. Plaga. Cryptographic protection of biometric templates: Chance, challenges and applications. In *BIOSIG*, pages 33–46, 2007.

[55] S. Lee, D. Moon, S. Jung, and Y. Chung. Protecting secret keys with fuzzy fingerprint vault based on a 3d geometric hash table. In *ICANNGA (2)*, pages 432–439, 2007.

[56] J. Li, X. Yang, J. Tian, P. Shi, and P. Li. Topological structure-based alignment for fingerprint fuzzy vault. In *ICPR*, pages 1–4, 2008.

[57] P. Li, X. Yang, K. Cao, P. Shi, and J. Tian. Security-enhanced fuzzy fingerprint vault based on minutiae's local ridge information. In *ICB*, pages 930–939, 2009.

[58] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, and J. Tian. An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *J. Network and Computer Applications*, 33(3):207–220, 2010.

[59] S. J. Lim, S.-H. Chae, and S. B. Pan. VLSI Architecture of the Fuzzy Fingerprint Vault System. In *ANNPR*, pages 252–258, 2010.

[60] D. N. C. Ling, A. T. B. Jin, and A. Goh. Biometric hash: high-confidence face recognition. *IEEE Trans. Circuits Syst. Video Techn.*, 16(6):771–775, 2006.

[61] R. Lumini and L. Nanni. An improved biohashing for human authentication. *Pattern Recognition*, 40:1057–1065, 2006.

[62] M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fern, J. Ortega-Garcia, and J. A. Siguenza. Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification. In *In: Proc. IEEE of International Carnahan Conference on Security Technology*, pages 151–159, 2006.

[63] J. Merkle, M. Niesing, M. Schwaiger, H. Ihmor, and U. Korte. Performance of the fuzzy vault for multiple fingerprints. In *BIOSIG*, pages 57–72, 2010.

[64] D. Moon, S. Lee, S. Jung, Y. Chung, M. Park, and O. Yi. Fingerprint template protection using fuzzy vault. In *ICCSA (3)*, pages 1141–1151, 2007.

[65] A. Nagar, K. Nandakumar, and A. K. Jain. Securing fingerprint template: Fuzzy vault with minutiae descriptors. In *ICPR*, pages 1–4, 2008.

[66] A. Nagar, K. Nandakumar, and A. K. Jain. Biometric template transformation: a security analysis. In *Media Forensics and Security*, volume 7541 of *SPIE Proceedings*. SPIE, 2010.

[67] A. Nagar, S. Rane, and A. Vetro. Alignment and bit extraction for secure fingerprint biometrics. In *SPIE Conference on Electronic Imaging 2010*, 2010.

[68] K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2(4):744–757, 2007.

[69] K. Nandakumar, A. Nagar, and A. K. Jain. Hardening fingerprint fuzzy vault using password. In *ICB*, pages 927–937, 2007.

[70] M. D. Raimondo, M. Barni, D. Catalano, R. D. Labati, P. Failla, T. Bianchi, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva. Privacy-preserving fingercode authentication. In *ACM MMSec'10*, 2010.

[71] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4):561–572, 2007.

[72] N. K. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur. Cancelable biometrics: A case study in fingerprints. In *ICPR (4)*, pages 370–373, 2006.

[73] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614–634, 2001.

[74] W. J. Scheirer and T. E. Boult. Cracking fuzzy vaults and biometric encryption. In *Proceedings of Biometrics Symposium*, pages 1–6, 2007.

[75] K. Simoens, J. Bringer, H. Chabanne, and S. Seys. A framework for analyzing template security and privacy in biometric authentication systems. *IEEE Transactions on Information Forensics and Security*, 7(2):833–841, 2012.

[76] K. Simoens, P. Tuyls, and B. Preneel. Privacy weaknesses in biometric sketches. In *2009 30th IEEE Symposium on Security and Privacy*, pages 188–203, May 2009.

[77] K. Simoens, B. Yang, X. Zhou, and F. Beato. Criteria towards metrics for benchmarking template protection algorithms. In *Proceedings of the 2012 5th IAPR International Conference on Biometrics*, march 2012.

[78] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar. Biometric encryption using image processing. In *Proceedings of SPIE*, volume 3314 of *Optical Security and Counterfeit Deterrence Techniques II*, pages 178–188, 1998.

[79] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar. *Biometric Encryption: ICSA Guide To Cryptography.* 1999.

[80] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and K. Vijaya. Biometric encryption: enrollment and verification procedures. In *Proceedings of SPIE*, volume 3386, pages 24–35. Optical Pattern Recognition IX.

[81] C. Soutar, G. J. Tomko, and G. J. Schmidt. Fingerprint controlled public key cryptographic system. US Patent, 5541994, 1996.

[82] A. Stoianov. Security issues of biometric encryption. In *Proceedings of the 2009 IEEE Toronto International Conference on Science and Technology for Hunanity (TIC-STH)*, pages 34–39, September 2009.

[83] A. Stoianov. Cryptographically secure biometric. In *SPIE Biometric Technology for Human Identification VII, volume 7667*, 2010.

[84] Y. Sutcu, H. T. Sencar, and N. Memon. A secure biometric authentication scheme based on robust hashing. In *Proceedings of the 7th workshop on Multimedia and security*, MM&#38;Sec '05, pages 111–116, New York, NY, USA, 2005. ACM.

[85] A. Teoh, A. Goh, and D. Ngo. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(12):1892–1901, Dec. 2006.

[86] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. Practical biometric authentication with template protection. In *5th Int. Conf. on Audio- and Video-Based Personal Authentication (AVBPA), Rye Brook, New York*, volume LNCS 3546, pages 436–446, Heidelberg, July 2005. Springer-Verlag Berlin.

[87] P. Tuyls, B. Škorić, and T. Kevenaar, editors. *Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting.* Springer-Verlag London, 2007.

[88] U. Uludag, S. Pankanti, and A. K. Jain. Fuzzy vault for fingerprints. In *AVBPA*, pages 310–319, 2005.

[89] M. V. D. Veen, T. Kevenaar, G. jan Schrijen, T. H. Akkermans, F. Zuo, and P. Holstlaan. Face biometrics with renewable templates. In *Proceedings of SPIE, Volume 6072: Security, Steganography, and Watermarking of Multimedia Contents VIII*, 2006.

[90] H. Xu, R. N. Veldhuis, T. A. Kevenaar, A. H. Akkermans, and A. M. Bazen. Spectral minutiae: A fixed-length representation of a minutiae set. *Computer Vision and Pattern Recognition Workshop*, 0:1–6, 2008.

[91] B. Yang, C. Busch, P. Bours, and D. Gafurov. Robust minutiae hash for fingerprint template protection. In N. D. Memon, J. Dittmann, A. M. Alattar, and E. J. D. III, editors, *Media Forensics and Security II*, volume 7541. SPIE, 2010.