Received February 11, 2016, accepted February 21, 2016, date of publication February 26, 2016, date of current version March 17, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2535120

Protection of Privacy in Biometric Data

IYNKARAN NATGUNANATHAN, ABID MEHMOOD, YONG XIANG, (Senior Member, IEEE), GLEB BELIAKOV, (Senior Member, IEEE), AND JOHN YEARWOOD
School of Information Technology, Deakin University, Geelong, VIC 3220, Australia

Corresponding author: Y. Xiang (yxiang@deakin.edu.au)

ABSTRACT Biometrics is commonly used in many automated verification systems offering several advantages over traditional verification methods. Since biometric features are associated with individuals, their leakage will violate individuals' privacy, which can cause serious and continued problems as the biometric data from a person are irreplaceable. To protect the biometric data containing privacy information, a number of privacy-preserving biometric schemes (PPBSs) have been developed over the last decade, but they have various drawbacks. The aim of this paper is to provide a comprehensive overview of the existing PPBSs and give guidance for future privacy-preserving biometric research. In particular, we explain the functional mechanisms of popular PPBSs and present the state-of-the-art privacy-preserving biometric methods based on these mechanisms. Furthermore, we discuss the drawbacks of the existing PPBSs and point out the challenges and future research directions in PPBSs.

INDEX TERMS Privacy protection, biometric data, automated verification system.

I. INTRODUCTION

With the advance of technology, automated identity verification has been implemented in many real-world applications, including granting access to shared computers, providing personal information at airports, allowing access to highly guarded areas such as nuclear facilities, and so on. Furthermore, because of the exponential growth of the Internet, identity verification becomes an essential part in web-based applications, such as online banking and online shopping. Traditionally, passwords, identity cards and pin numbers are used for the verification of individuals. These knowledge and token based schemes have several disadvantages. For example, a pin number can be shared by many people and an identity card can be stolen by someone. Moreover, attackers can get access to a system by guessing passwords and pin numbers or disable the system by intentionally supplying the incorrect information several times.

In order to overcome the issues in traditional verification methods, human biological characteristics have been exploited to develop biometric based verification systems. Biometric verification is defined as the verification of an individual based on the physical, chemical or behavioral attributes of the person [1]. The biometric traits which can be used for verification include fingerprints, face, voice, iris and keystroke pattern. The main advantage of using biometric traits in identity verification systems is that they cannot be easily shared or stolen. In addition to this, biometric schemes are easier to use, as users do not need to remember passwords, pin numbers or carry their identification cards.

Although the biometric based verification systems have obvious advantages over the traditional ones, such systems can risk the privacy of individuals if they are not designed appropriately. For example, a biometric system may store fingerprints or iris data. If the biometric data is exposed to an attacker, the latter can be used for undesired purposes such as impersonation. More importantly, since the biometric data is derived from the biological characteristics of individuals, they cannot be altered. Thus, the leakage of the biometric data can cause serious and continuous threats to the privacy of individuals. Therefore, the biometric data should be protected in such a way that even if it is compromised, the attacker still cannot gather any information which can breach individuals' privacy. Besides, an attacker should not be able to login as a genuine user.

In order to protect the biometric data which contains individuals' privacy information, some privacy-preserving biometric schemes (PPBSs) have been developed in recent years. These PPBSs can be classified into biometric encryption based schemes, cancelable biometric based schemes, multi-modal and hybrid based schemes, and secure computation (SC) based schemes. Biometric encryption refers to associating a digital key with biometric data. This can be done by binding the key with the biometric data or generating the key from the biometric data [2]. Cancelable biometrics involves using and storing intentionally distorted or transformed biometric features extracted from biometric signals in the biometric related applications. The utilization of purposely altered biometric signals reduces the risk of exposing the contents of the original biometric data [3]. While multi-modal based schemes use more than one biometric traits (e.g., iris and voice signals) for verification, hybrid based schemes are developed by combining PPBSs such as a biometric encryption based scheme and a cancelable biometric based scheme. With respect to the SC based methods, they guarantee high level of privacy of biometric data by using encryption techniques such as homomorphic encryption and garbled circuits.

Privacy-preserving biometric verification is a very active research area and has been progressing fast over the last few years. Recently, some survey/review type of papers about privacy-preserving biometrics have been published in the literature [4]–[15]. However, while these papers introduced the general concept of privacy-preserving biometrics and some PPBSs from different aspects, their scopes are limited. For example, Belguechi *et al.* [4] neither discussed the popular PPBSs based on cryptographic techniques nor provided detailed discerption of cancelable biometrics. In [5], there was no mentioning of the robustness against attacks and the tradeoff between the level of privacy and false acceptance rate (FAR). Rane *et al.* [6] only very briefly mentioned the possible attacks and performance measures but some important PPBSs, such as hybrid PPBSs, were not included. Similarly, Nandakumar and Jain [7] did not give details about the schemes under the template protection category and the SC based schemes. Compared with [4]–[7], the scopes of [8]–[15] are even narrower. They only focus on some specific issues in privacy preserving biometrics, such as privacy preserving multi-modal biometrics [8], SC [9], error control mechanisms related to PPBSs [10], adversarial machine learning [11], biometric feature preprocessing [12], spoofing attack [13], cancelable biometrics [14] and biometric signal processing in encrypted domain [15].

Moreover, while standardization is an important issue in privacy-preserving biometrics, it was not discussed in [4], [5], and [7]–[15]. Although standardization is briefly mentioned in [6], the problems and challenges encountered in standardization were not illustrated. Furthermore, the papers [4]–[6], [8]–[11], and [15] did not discuss in detail the current challenges and future research directions in this research area. The papers [7] and [12]–[14] only discussed challenges and research directions in several specific subareas, e.g., challenges in biometric features [12] and robustness enhancement of cancelable PPBSs [14].

In this paper, we will give a comprehensive and up-to-date overview of the popular and state-of-the-art PPBSs using a generic framework. The shortcomings of these PPBSs will be summarized and discussed, with particular focuses on the robustness against attacks, the contradictory requirements of privacy and accuracy, and the problems in standardization. Furthermore, we will show the major challenges and project the potential future research directions in PPBSs. We will also suggest possible techniques to tackle these challenges and handle future demands. Compared with [4]–[15], our paper contains a number of unique and novel aspects, including

- much more comprehensive and up-to-date coverage of the state-of-the-art PPBSs,
- detailed discussions of the problems in existing PPBSs, where standardization is particularly highlighted, and
- detailed discussions of the challenges and future research directions in PPBSs, together with suggested techniques to tackle these challenges.

The remainder of the paper is organized as follows. The basic framework and performance evaluation measures of PPBSs are presented in Section II. In Section III, we categorize PPBSs and present a detailed discussion about each category. The drawbacks of the existing PPBSs are summarized and discussed in section IV, in terms of robustness, level of privacy versus FAR, and standardization. Section V show the challenges and future research directions in PPBSs, together with suggested techniques to tackle these challenges, and Section VI concludes the paper.

II. BASIC FRAMEWORK AND PERFORMANCE MEASURES OF PPBSs

A. BASIC FRAMEWORK

The main motivation behind PPBSs is to preserve the privacy of a user while maintaining the verification accuracy. An effective and practical biometric system should exhibit two important characteristics: irreversibility and unlinkability. Irreversibility means that it should be difficult to reconstruct the original biometric signal from the stored data available to public. Unlinkability refers to the ability to create many uncorrelated versions (or transforms) of the original biometric signal. Wang *et al.* proposed a general framework for PPBSs [16], which includes two parts: enrolment and verification. This framework is applicable to most of the existing PPBSs.

1) ENROLMENT

At the enrolment stage, a user provides a biometric signal as an input. The important features of the biometric signal are extracted using a feature extraction module. We denote the extracted biometric features set by x. In order to protect the privacy of biometric data, x will not be stored in a database. Instead, x is processed in certain ways to produce the so-called helper data, denoted by v. The helper data v is stored in a database and plays an essential role at the verification stage. This process should be designed in such a way that it is almost impossible to retrieve x from v, which greatly protects the privacy of biometric data. In these PPBSs, only the biometric sample is required to perform identity verification at the verification stage. On the other hand, some PPBSs employ a secret key s_k, in different manners, to further enhance the protection of biometric data privacy. In some cases, the altered version of the secret key $h(s_k)$ is also stored in the database. In PPBSs, where secret key is used in addition to biometric signals are known as two factor verification schemes, where both the biometric sample and the secret key are needed at the verification stage.

2) VERIFICATION

At the verification stage, the received biometric signal, together with the secret key in the case of two factor verification schemes, is used to extract the biometric features and then produce the helper data. We denote the biometric feature set and helper data obtained at the verification stage by x' and v', respectively. Based on the similarity between v' and its counterpart v obtained at the enrolment stage and stored in the database, one decides whether a legitimate user or an adversary is present. In some schemes, at the verification stage, a secret key s'_k is generated from the received biometric signal and the stored helper data. Then the altered version of the generated secret key $h(s'_k)$ is obtained. For verification, $h(s'_k)$ and its counterpart $h(s_k)$ are compared. Dodis *et al.* [17] defined three metrics to compare the similarity between two binary vectors: Hamming distance metric, set difference metric and edit difference metric. These metrics are detailed as follows:

- Hamming distance metric: The hamming distance between two vectors V and V' (both represented in binary form), denoted by $\mathrm{dis}(V, V')$, is the number of positions at which the strings V and V' differ.
- Set difference metric: The set difference distance between two subsets V and V' is defined as
$$\mathrm{dis}(V, V') = |V| + |V'| - 2|V \cap V'|$$
where $\cap$ stands for intersection operation and $|A|$ denotes the size of A.
- Edit difference metric: The edit difference distance between V and V' is the minimum number of insertions and deletions needed to convert V into V'.

For example, if $V = [1, 0, 0, 1, 1, 0, 1]$ and $V' = [1, 1, 0, 1, 1, \ 1, 0]$, the related Hamming distance and edit difference distance can be directly obtained from their definitions as 3 and 6, respectively, and the set difference distance can be calculated as $|V|+|V'|-2|V \cap V'| = 7+7-2\times4 = 6$.

It should be noted that the majority of biometric verification schemes normally either use hamming distance or set difference distance. This is because biometric features or their altered counterparts can always be represented as either a binary string (e.g., iris codes) or a set of features (e.g., minutiae points for fingerprints).

B. PERFORMANCE MEASURES

PPBSs could suffer from noise in the received biometric signal, as the recordings of the same biometric signal recorded at different times and under different conditions may vary significantly. Incorrect decisions may come from the unsuccessful genuine attempts or the successful imposter attempts. The following measures are used to asses the accuracy of a PPBS system, i.e., how reliably a system verifies a genuine user and rejects an impostor:

- *False rejection rate (FRR):* FRR is the probability that the system rejects a genuine user. It is also called the probability of missed detection.
- *FAR:* FAR or false acceptance rate is the probability that the system verifies a probe biometric signal which comes from a person different from the enrolled identity. It is also called the probability of false detection. For any given biometric system, there exists a trade-off between FAR and FRR.
- *Equal error rate (EER):* EER is a value used to express the performance of a biometric system. For a given biometric system, FRR and FAR are inversely related and by adjusting the system parameters, either FRR or FAR can be reduced at the expense of the other. In order to represent the performance of a given system quantitatively by a single value, EER is defined as the point at which FAR is equal to FRR. EER should be as low as possible for biometric systems.
- *Successful attack rate (SAR):* SAR is the probability that the system authenticates an adversary instead of a legitimate candidate, where the adversary is aided by some side information consisting of the stored helper data and/or the secret key. The SAR is always greater than or equal to FAR as additional information improves the adversary's ability to falsely authenticate him/her.

Regarding the performance of PPBSs in relation to privacy, the commonly used measures are as follows:

- *Privacy leakage:* Privacy leakage refers to the leakage of information about the biometric signal when the stored helper data is compromised.
- *Non-invertibility:* Non-invertiblity refers to the inability to reconstruct the biometric features from the helper data. It can be measured by the conditional Shannon entropy of the biometric features given the helper data. In the context of biometric encryption based schemes, the amount of information which helper data reveals about the biometric features is referred as entropy loss. Entropy loss is a useful measure to compare different PPBSs [7].
- *Revocability and non-linkability:* Revocability refers to the renewability of helper data in case it has been compromised. Non-linkability refers to preventing cross matching of helper data across different applications. Although many PPBSs claim to have the revocability and non-linkability properties, the analysis in [16] shows these schemes do not satisfy the condition of revocability and non-linkability.

In addition to the above measures related to accuracy and privacy, Computational complexity and storage requirement are also important to a PPBS. These measures are outlined below:

- *Computational complexity:* Computational complexity can be measured by means of the required resources (e.g., processor speed, memory, disk space, etc.) and processing time. It plays an important role in determining the usability of a PPBS.

- *Storage requirement:* Storage requirement refers to the number of bits required to store the helper data and/or the secret key.

III. PRIVACY PRESERVING BIOMETRIC SCHEMES

Over the last decade, many PPBSs have been developed to protect the privacy of biometric signals. These schemes can be broadly grouped as biometric encryption based schemes, cancelable biometric based schemes, multi-modal and hybrid based schemes, and SC based schemes.

A. BIOMETRIC ENCRYPTION BASED SCHEMES

Biometric encryption originated from the idea of protecting the privacy of a biometric signal by encrypting it using a cryptographic technique. This leads to very low level of FAR and thus makes the biometric systems more secure from hackers. The major problem in combining biometrics with cryptography is the inherent variation of biometric features, which is caused by the imperfect nature of biometric feature extraction and matching algorithms. Since it is difficult to produce exactly the same biometric features at the verification stage, the exact matching of biometric features is usually impossible. Due to this reason, the standard cryptographic approaches cannot be used in biometric verification systems directly. To cope with the variation in biometric features, fuzzy based techniques were introduced into biometric verification systems.

In the enrolment process, a discrete feature set is extracted from the original biometric signal and a secret key is combined with the biometric feature set through a binding algorithm. The resulting representation and the hash value of the key are stored in the database but the biometric feature set and the key are discarded. Binding should be performed in a secure way such that neither the key nor the biometric information can be retrieved, even when the stored data is compromised. In the verification process, if the presented biometric signal is sufficiently close to the stored biometric data, the original secret key can be retrieved and the user can be authenticated based on that. The levels of privacy and verification accuracy rely on the length of the secret key and the encryption algorithm [18]. The major challenge between binding and retrieval of the algorithm is to bridge the gap between the fuzziness of biometric and the exactness of cryptography.

The operation of biometric encryption can be classified into two modes: key binding mode and key generating mode.

1) KEY BINDING MODE BASED SCHEMES

In the key binding mode, a randomly generated secret key and the biometric features are combined monolithically using cryptographic framework. In other words, the secret key is encrypted using biometric features. The biometrically encrypted data (which is the helper data in this context) and the hash value of the secret key are stored. At the verification end, the secret key is retrieved using the stored biometrically encrypted data and the received biometric signal. During the verification process, the hash value of the retrieved secret key is compared with the stored hash value of the secret key.

Many PPBSs are based on the biometric key binding mode [19]–[35]. In the early days, two PPBSs called Mytec1 and Mytec2 were proposed [19], in which an altered feature set is generated from biometric signals using a random array. Then, this altered feature set is linked with a secret key to create a lookup table. At the enrolment stage, the lookup table, the hash value of the secret key and the details about the random array are stored. These stored data together with the received biometric signal are used for verification. The major drawback of Mytec1 and Mytec2 is their poor verification accuracy, caused by their high sensitivity to noise. For the PPBSs in [20]–[35], they take advantage of either fuzzy vault or fuzzy commitment based techniques.

Key Binding Mode Based PPBSs Using Fuzzy Vault: Fuzzy vault is a popular error resistant technique initially proposed by Jules and Sudan [20]. It is designed to work with unordered sets (e.g., important feature points, known as minutiae points, in fingerprints) and has the ability to deal with interclass variation which is commonly encountered in biometric data. Fig. 1 illustrates the basic key binding mode based PPBS using fuzzy vault. First of all, from the biometric signal such as a fingerprint, a biometric feature set x is extracted. Besides, based on the secret key s_k, a corresponding polynomial p is generated, e.g., the elements of s_k could be used to form the coefficients of p. Then, the projection of the unordered biometric feature set x on the polynomial p is calculated. After that, the random points which do not lie on the polynomial p, called chaff points, are added to the calculated projected points. Denote both sets of points (i.e., the projected points on the polynomial and the added chaff points) as v. In a PPBS using fuzzy vault, the helper data v is popularly known as the vault. Here, the chaff points are added to conceal the polynomial p from an attacker. In addition to v, the hash value of the secret key, denoted as $h(s_k)$, is also stored during the enrolment process. At the verification stage, to successfully unlock the vault v, a set of biometric features x' is needed. If the received biometric feature set x' largely overlaps with x, one can locate adequate number of points in v, which lie on the polynomial p. From p, the secret key s'_k can be extracted. Finally, verification is done by comparing the hash value of the derived secret key, $h(s'_k)$, and the stored $h(s_k)$.

The first working key binding mode based PPBS using fuzzy vault was introduced by Clancy *et al.* [21], where the pre-aligned feature set from fingerprints was assumed. Due to this assumption, the practicality of this method is very limited. To remove this assumption, Nandakumar *et al.* introduced a method utilizing the high curvature points derived from the orientation field of fingerprints [22]. Differently, to overcome the alignment issue, Li *et al.* proposed to fuse the local features and local structures to withstand geometric transformations such as rotation and translation [23]. In [24], the orientation information of the biometric data was employed to increase verification accuracy. While verification accuracy can also be improved by

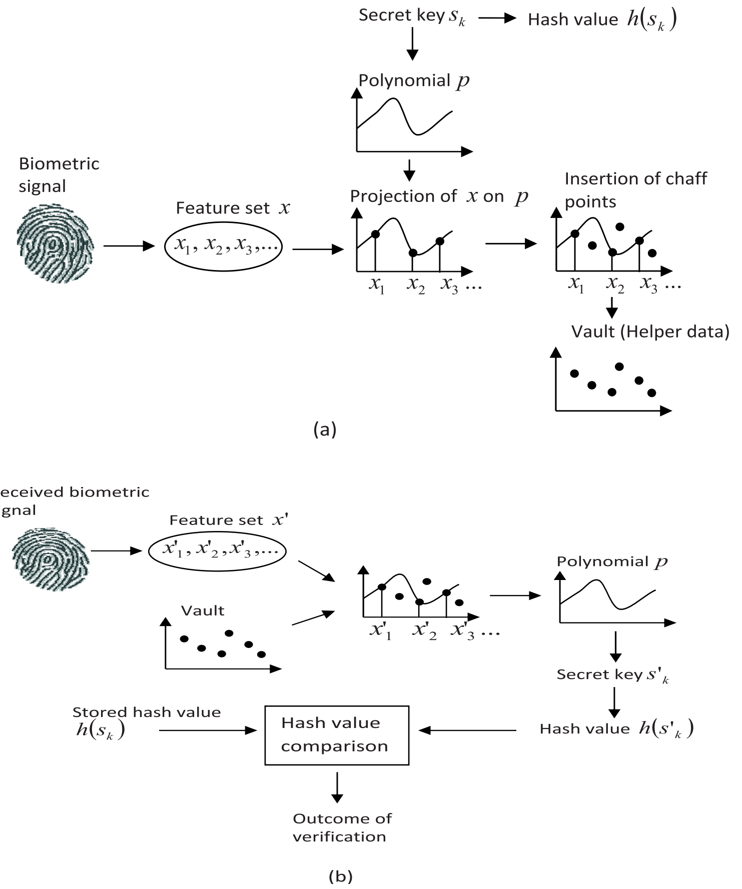


FIGURE 1. **Illustration of basic key binding mode based PPBS using fuzzy vault. (a) Enrolment; (b) Verification.**

increasing the number of chaff points, the increase of chaff points will inevitably raise computational complexity. In [25], Nguyen *et al.* proposed a mechanism to generate chaff points in a faster and more efficient way. It is worth mentioning that although the PPBSs using fuzzy vault were initially applied to fingerprints, they are also applicable to other biometric signals such as iris [26], palmprints [27], and face biometrics [28].

Key Binding Mode Based PPBSs Using Fuzzy Commitment: The basic key binding mode based PPBSs using fuzzy commitment was reported in [29] and Fig. 2 shows its block diagram. In the enrolment process, the biometric feature set x and a secret key s_k are used as two input components, where s_k is usually a codeword generated using an error correction code. From x and s_k, a difference vector v (i.e., the helper data) is computed in certain way. For example, v can be obtained using the XOR operation, i.e., $v = s_k \oplus x$, where $\oplus$ denotes XOR operation. The obtained difference vector v is stored in the database, together with the hash value of the codeword, $h(s_k)$. At the verification end, the codeword is generated using the received biometric signal and the stored difference vector v. Then, the verification is done by comparing the hash value of the generated codeword and the stored counterpart.

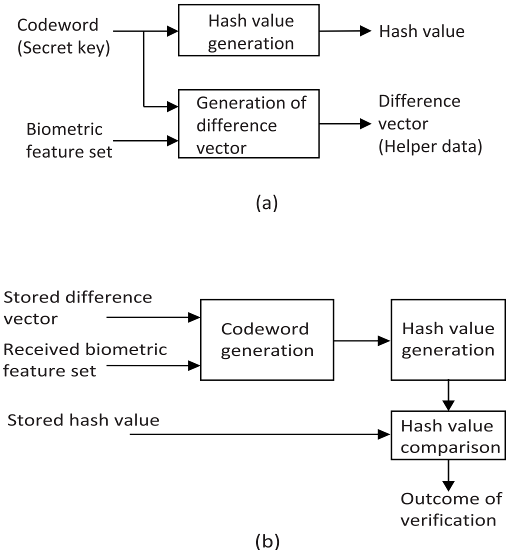


FIGURE 2. **Block diagram of basic key binding mode based PPBSs using fuzzy commitment. (a) Enrolment; (b) Verification.**

Many modifications have been made to the basic fuzzy commitment based PPBS to improve performance. Bringer *et al.* used two-dimensional iterative min-sum code and binary Reed-Muller code to improve the efficiency of the decoding process [30]. In [31], the context-based reliable component selection is used to extract the secret key from iris-codes. In [32], the randomized dynamic quantization transformation is utilized to create the binary form of the fingerprint features and the Reed-Solomon code is employed to improve the decoding performance. In [33], Nandakumar used the focal points of high curvature regions to obtain alignment in fingerprint features and used a binary fixed-length feature representation. In addition to iris fingerprint, the fuzzy commitment concept is also applied in other biometrics such as face biometrics [34] and online signatures [35]. Since the fuzzy commitment based PPBSs normally use relatively shorter codewords, they are relatively vulnerable to brute force attack, which guesses the codewords through exhaustive search.

2) KEY GENERATING MODE BASED SCHEMES

In the key generating mode, the secret key is generated directly from a biometric feature set. While it appears to be a simple and attractive proposition, its implementation is challenging as it requires high key stability and entropy. Here, key stability refers to the ability of repeatedly generating the same key from a given biometric signal and key entropy relates to the number of possible keys which can be generated. Since biometric signals are sensitive to noise, it is difficult to maintain high key stability. Having high key stability and entropy simultaneously is even more difficult as key stability and key entropy are inversely related.

One type of key generating mode based PPBSs employed the concept of user specific quantization methods [36]. In [37], Chang *et al.* proposed a method for stable key generation from biometric signals. In particular, a collection of biometric features of an authentic user is used to register the user, where the user specific feature transform is conducted in such a way that the transformed feature space of the authentic user is compact while those of the impostors are diverse. In this way, the transformed feature space of the authentic user is distinguishable from those of the imposters and each feature can contribute to one or more bits of information into the cryptographic key generation process. This helps in making long and stable keys. More key generating mode based PPBSs employing the user specific quantization methods can be found in [38]–[40].

Another type of key generating mode based PPBS utilized fuzzy extractor [17] and Fig. 3 shows its block diagram. In the enrolment process, the biometric feature set x and a seed are considered as inputs. From x, the helper data v is produced via a mechanism known as secure sketch. This mechanism involves the quantized random projections of x and an error correction code with parity check matrix. In addition, from x and the seed, a uniform random string s_k is generated using a random extractor, where s_k acts as a secret key. The helper data v and the hash value of the secret key, $h(s_k)$, are stored in the database. At the verification stage, one first extracts x' from the received biometric signal, which is often noisy.

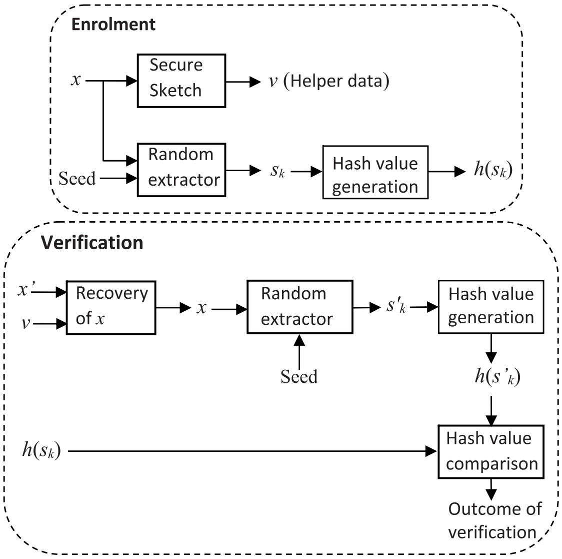


FIGURE 3. Block diagram of key generating mode based PPBS using fuzzy extractor.

Then, the original feature set x is recovered by exploiting x' and v. Based on x and the seed, a random extractor can be applied to generate the secret key s'_k and then its hash $h(s'_k)$ is computed. Finally, verification is performed by comparing $h(s'_k)$ with $h(s_k)$. In [17], the fuzzy extractors were constructed using three metrics: Hamming distance, set difference and edit distance.

While the PPBSs using fuzzy extractors usually require less storage space than other PPBSs do, they have some disadvantages. Firstly, fuzzy extractors cannot be reused multiple times for the same biometric signal due to their low key entropy, which significantly reduces their usability in practice [41], [42]. Secondly, fuzzy extractors are vulnerable to the uncertainty in the biometric signal, especially in the case of fingerprints, and the misalignment in the received biometric signal [43]. Thirdly, significant identity information leakage could occur in fuzzy extractors [44].

B. CANCELABLE BIOMETRIC BASED SCHEMES

Cancelable biometrics refers to adding a repeatable distortion to the biometric signal systematically and intentionally, in order to protect the user's privacy [3]. The distortion is controlled by some parameters derived from a secret key, where the secret key can be a pseudo random number, a password or some other random key. The helper data v is created by applying the distortion to the biometric feature set x and stored in the database. Following the approach used in the enrolment process, one can perform verification by creating v' from the received biometric feature set x' and then comparing the generated v' with the stored v. If the helper data v is compromised, the distortion parameters can be changed to generate a new set of helper data. The distortion functions are designed in such a way that it is computationally difficult for an adversary to recover the original biometric feature set x. Among the existing cancelable biometric based schemes, most of them exploit either biohashing or non-invertible transform.

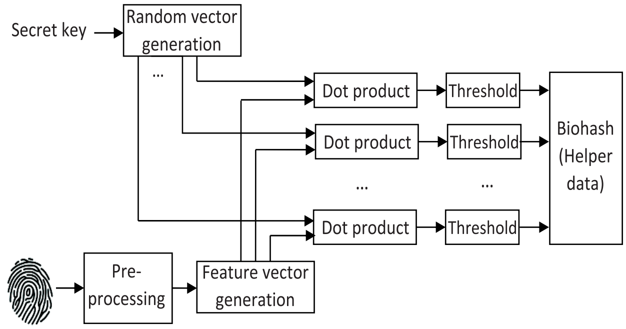


FIGURE 4. **Block diagram of generating biohash value.**

1) CANCELABLE BIOMETRIC BASED PPBSs USING BIOHASHING

A biohashing process consists of two steps. In the first step, a preprocessing is carried out on the biometric feature set in order to make the biometric feature invariant to small variations in the input biometric signal. For example, in the case of face biometrics, Fourier-Mellin transform can be used to make the feature vector invariant to geometric variations such as rotation and translation. In the second step, a user specific secret key is used to generate a random vector. Then, a biohash value is generated by comparing the inner product of the generated random vector and the feature vector extracted against a predefined threshold. Fig. 4 shows the block diagram of generating biohash value. At the verification end, by following the process used at the enrolment stage, a biohash value can be generated from the received biometric signal and the secret key given by the user. Afterwards, the verification is done by comparing the newly computed biohash value with the stored biohash value. Some representative PPBSs based on biohashing can be found in [45]–[47].

In a PPBS using biohashing, the user defined secret key increases the entropy of the biometric feature set. It is almost impossible to reconstruct the original biometric feature set without knowing the secret key. This is primarily due to the usage of dot product and the threshold based mechanisms [48]. Although the aforementioned PPBSs using biohashing offer good privacy preservation, they have a major issue, which is that a person stealing the secret key is able to compromise the system. As shown in [49], when biohashing is operated under the hypothesis of stolen secret key, the system performance in terms of FAR moves form 7.3% to 10.3%. To address this issue, Lumini *et al.* proposed several solutions for augmenting the length of the secret key [50]. Besides, in [51], Nanni and Lumni used the invariant local binary pattern texture operator for fingerprints to improve verification accuracy [51]. However, since this approach utilizes minutiae comparator for alignment, it results in lower level of privacy.

2) CANCELABLE BIOMETRIC BASED PPBSs USING NON-INVERTIBLE TRANSFORM

In a cancelable biometric based PPBS using non-invertible transform, the biometric feature set is secured by applying a non-invertible transformation function [52]. The non-invertible transform refers to a one-way function, $F(x)$, which is easy to compute (in polynomial time) but difficult to invert.[1] The parameters of the transformation function are defined by a secret key which must be available at the time of verification. The main characteristic of this approach is that even if the secret key or/and the transformed feature set are known, it is computationally challenging, in terms of brute force complexity, for an adversary to recover the original biometric feature set. During the enrolment process, the transformed biometric feature set, i.e., the helper data v, is stored in the database. At the verification stage, the received biometric features and the secret key are exploited to generate the transformed feature set v', and then v' is compared with the stored counterpart v for verification. It should be noted that in a PPBS using non-invertible transform, non-invertibility and verification accuracy are two contradictory requirements [53].

Various transforms have been used in PPBSs and their impact on verification accuracy is investigated. In [52], Ratha *et al.* compared cartesian, polar and surface folding transforms in the context of the minutiae positions for fingerprints. It is shown that the verification system performance under transformation remains almost the same as without transformation while maintaining the irrevocability. It is further revealed [54] that in Ratha's surface folding transform based mechanism, the original biometric feature set can be regenerated when the transformed biometric feature set and the secret key are known. In [55], Teoh *et al.* proposed a cancelable formulation, where the biometric feature set is first distorted in a revocable manner using a non-inventible transform. Then, the distorted feature vector is projected onto random subspaces using a user-specific pseudo random number which acts as a secret key. Regarding the performance perspective, three different scenarios were considered: normal, stolen pseudo random number and compromised distorted feature vector. In [56], Wang *et al.* proposed a mechanism to transform the original biometric feature set using random transforms, including random additive transform, random multiplicative transforms and random projections. The random transforms in combination with sorted index numbers approach satisfy the condition of revocability and non-invertibility. Hence, among the transforms considered, the random transforms provide greater level of privacy. Furthermore, adaptive bloom filters were utilized in [57] achieve efficient and alignment-invariant biometric comparison, which is also irreversible, with particular focus on iris verification.

[1] Given $F(x)$, the probability of finding x in polynomial time is very small.

C. MULTI-MODAL AND HYBRID BASED SCHEMES

Achieving high verification accuracy is a primary objective for all PPBSs. Intuitively, using more than one biometric trait would be beneficial to improve verification accuracy, which leads to multi-modal and hybrid based PPBSs.

1) MULTI-MODAL BASED PPBSs

As shown in [58], combining two biometric traits, e.g., ear and face, face and fingerprint, etc. help deal with problems like intra-class variability, inter-class similarity, data quality and sensitivity to noise. Solving or moderating these problems in return improves verification accuracy. By combining diverse biometric traits in different ways, various multi-modal based PPBSs have been developed. The PPBS in [59] combines fingerprint and voice using fuzzy logic. In [60], face and online handwritten signature were combined using linear discriminant analysis. To ensure that the significant features were used in a balanced manner, a genetic algorithm with modified fitness function was utilized in [60]. In [61], Nadheen *et al.* employed principle component analysis to extract features from ear and iris, and the extracted biometric features were jointly exploited using the score level fusion. More multi-modal based PPBSs can be found in [62] and [63].

2) HYBRID BASED PPBSs

In PPBSs, both biometric encryption and cancelable biometrics have their own pros and cons. The underlying idea behind the hybrid concept is to combine different schemes appropriately to take advantages of their strengths. For example, one type of cancelable biometric based PPBSs use a non-invertible transform function to transform the biometric feature set and do verification comparison in the transformed domain. The drawback of these schemes are that the transformation sometimes tends to break the underlying structure, as in the case of fingerprints, thus reducing the verification accuracy. On the other hand, a fuzzy extractor uses error correction code to recover a uniform random string with the assistance of helper data. The problem with fuzzy extractor is that the error correction code reduces the verification accuracy. To get the best of both approaches, one can apply the error correction techniques in fuzzy extractor to cancelable biometric based schemes to get better verification performance [63]. More hybrid based PPBSs are shown in [64]–[67], aiming to better protect the privacy of biometric feature set and to increase the verification accuracy.

D. SC BASED SCHEMES

As shown in the above subsections, most PPBSs such as those based on biometric encryption and cancelable biometrics achieve biometric feature protection at the cost of lowering verification accuracy. Differently, SC based PPBSs aim to protect biometric feature set at the expense of high computational complexity and storage requirement. This is achieved by doing computations in an encrypted domain. Depending on the application scenarios, the computation result can be a boolean value, the index of a closest element, or a probabilistic measure of the similarity (or dissimilarity) between encrypted feature sets. Compared with biometric encryption and cancelable biometric based PPBSs, SC based PPBSs can achieve higher level of privacy and verification accuracy as they utilize well-established encryption algorithms. They are particularly useful in some applications, such as in large scale verification systems where the client and server engage in a biometric verification process but not reveal to each other any biometric data. However, their usage in most real life applications is prohibited due to their high computational complexity and storage requirement. While different techniques have been used in SC based PPBSs, homomorphic encryption and garbled circuit are two representative ones.

1) SC BASED PPBSs USING HOMOMORPHIC ENCRYPTION

Homomorphic encryption was first introduced by Rivest *et al.* in 1978 [68]. In SC based PPBSs using homomorphic encryption, the biometric feature set is encrypted using homomorphic encryption via a public key. The public key is only used for encryption and it cannot be employed for decryption. The encrypted biometric feature set is stored in a data base. During the verification phase, the biometric feature set of the received biometric signal is extracted and then encrypted using the public key. Verification is conducted by comparing the similarity, by means of a distance matrix, between the received encrypted feature set and the stored encrypted feature set. A privacy-preserving comparison protocol is used to determine whether the distance is below a threshold or not and only the verification system knows the threshold. Due to the usage of homomorphic encryption, the similarity between the biometric signals used in enrolment and verification processes is reflected in their encrypted counterparts. This is vital as the biometric feature sets used in enrolment and verification processes are not going to be identical due to noise and misalignments. Several more recent homomorphic encryption methods were reported in [69]–[72].

There were also verification applications, in which partially homomorphic encryption was used. A system is considered as partially homomorphic, if it exhibits either additive or multiplicative homomorphism, but not both [69]. The most popular form of partially homomorphic encryption is Paillier cryptosystem, which possesses additive homomorphism. In order to improve verification accuracy and privacy, Paillier cryptosystem is also used together with other multiparty computation techniques. For example, in the Scifi project [73], Paillier cryptosystem and another SC technique called oblivious transfer [74] are used to implement a face identification system under secure computation. However, the current Paillier cryptosystem is in general very slow, limiting its applications in practice.

2) SC BASED PPBSs USING GARBLED CIRCUIT

In a biometric based verification system, a large amount of helper data corresponding to different users is often stored in the database. If the system wants, it can track or monitor a user's activity with respect to verification. For example, if a user verifies his identity at different branches of a particular bank, the verification system may determine the user's geographic location to a certain extent. The garbled circuit can be used to deal with this issue. The garbled circuit theory was introduced by Yao in 1986 [75] and has been commonly used in private computing. It allows the evaluation of binary circuits, such as the circuits made up by AND and OR gates, on inputs privately owned by two parties involved in the computation. The result of the evaluation is made available to either one or both parties while the intermediate values cannot be discovered by any of them. The inherent nature of garbled circuit enables it to prevent the verification system from knowing which helper data is compared. Consequently, the system does not know who is doing the verification.

Blanton *et al.* proposed a privacy-preserving protocol for iris and fingerprint matching [76], in which the garbled circuit concept was exploited. In [77], Chun *et al.* presented another garbled circuit based protocol for biometric authentication. The protocol in [77] is secure in the honest-but-curious model but its performance in computation is not satisfactory as it takes a relatively long time for execution.

IV. MAJOR PROBLEMS IN EXISTING PPBSs

In this section, we analyze the major problems of the existing PPBSs in terms of robustness, level of privacy versus FAR, and standardization.

A. ROBUSTNESS

Over the last few years, PPBSs have become a vital part of information security systems due to the increasing demand of privacy protection. A PPBS should not only protect the privacy of biometric data but also ensure very high verification accuracy, i.e., verifying the legitimate users and resisting any attempts by imposters to get unauthorized access. PPBSs could be attacked by attackers in various ways, aiming to either get authenticated fraudulently or to compromise the user privacy [78], [79]. Although the existing PPBSs were designed to resist as many attacks as possible, they do not have adequate successful verification rate under popular attacks.

The attacks on biometric verification systems can be classified in many ways. By considering the sources of attacks and the attackers' goals, the major attacks on privacy-preserving biometric verification systems can be categorized as follows.

- *FAR attack:* In biometric based verification systems, false acceptance occurs due to interclass correlation, i.e., the features extracted from two different biometric signals using a given algorithm may have similar characteristics. For example, if a system has a false acceptance rate of 0.01%, it means that it is possible to get unauthorized access if 10^4 trials are carried out to compare the features from different users. Therefore, an attacker who has access to a large biometric database can exploit this property to attack a verification system. Such attack is called FAR attack.
- *Linkage attack:* The advantage of using biometric feature set for verification is that it creates a direct connection between a user and his/her identity. However, if a user is registered on different verification systems using the same biometric trait, the user's activities could be traced online [80]. Linkage attack aims to compromise the user's privacy by cross-matching the helper data related to the user but stored in different system databases.
- *Hill climbing attacks:* The hill climbing attack can be exerted on the biometric verification systems which reveal the matching level between the received biometric feature set and the stored helper data. For example, in a face based verification system, if information about the similarity score between the received face image and its stored counterpart is somehow disclosed, it is possible for an attacker to regenerate the face image using a recursive scheme [81].
- *Brute force attack:* Brute force attack, basically an exhaustive search on all possible combinations of keys or passwords, is theoretically able to crack any verification system which depends on encrypted data. To launch this attack, massive amount of computational power is needed. As an example of brute force attack, it was used to crack fuzzy vault [82], with which the secret key could be recovered.

B. LEVEL OF PRIVACY VERSUS FAR

The main objective of PPBSs is to preserve the privacy of users while ensuring lower FAR. Many studies have been conducted to investigate the level of privacy against FAR from an information theoretic prospective [83]–[85]. These studies show that in the existing PPBSs, higher level of privacy is often achieved at the cost of increasing FAR. For example, the biometric encryption based PPBSs usually obtain lower FAR by increasing the size of the secret key as it is hard for an attacker to guess the key with longer length [86], [87]. However, on the other hand, a longer key length could decrease the level of privacy, because the helper data generated using a key with longer length could contain more information about the original biometric signal. Thus, there is a tradeoff between privacy and FAR.

C. STANDARDIZATION

In recently years, PPBSs have been attracting more and more attentions from researchers in academia and industry. From the view point of system implementation, the enrolment module of a typical PPBS includes sensors, quality assessment and feature extraction units and its verification module contains feature extraction, matching and decision making units. Since there are a range of modules and units involved in the implementation of the PPBS, the compatibility among these modules and units is very important. This inevitably makes standardization an essential part in PPBS design and implementation.

Standardizing biometric information protection was first mentioned in ISO/IEC 24745 [88], which gave general guidance on low FAR and privacy-compliant management and processing of biometric information. This standardization divides the stored data in the enrolment phase of a biometric verification system into auxiliary data and a pseudonymous identifier. Here, the auxiliary data denotes helper data and the pseudonymous identifier commonly refers to an altered version of the secret key. ISO/IEC 24745 also lists the potential attacks on the biometric verification systems, such as data hacking during the data transfer between different modules. Furthermore, it gives directions on the implementation of PPBSs, including the way of storing data and the communication between different modules. In relation to privacy aspect, ISO/IEC 24745 defines irreversibility, unlinkability and confidentiality, in order to ensure that the users' biometric features do not go to the hands of an unintended person or an attacker.

The standardization of performance metrics and assessment methodologies was addressed in ISO/IEC 19795 [89]. It defines performance metrics such as FAR and FRR. Recently, the standardization of performance testing of biometric verification schemes has been defined in WD 30136 [90]. The performance metrics related to handling different PPBSs, such as privacy leakage and successful attack rate, have also been defined in WD 30136.

Although there are attempts to standardized modules in PPBSs, this standardization process is in the early stage. More comprehensive and generalized frameworks should be developed to standardize various modules in PPBSs. This will surely assist the industrial deployment of PPBSs by providing compatibility among different modules in biometric schemes. The main problems associated with the standardization of biometrics can be summarized as follows.

- Since there are many different schemes used in privacy preserving biometric systems, it is difficult to enforce standardization.
- The involvement of various parties, such as manufacturing industries, security agencies and research institutes, makes it hard to implement standardization within a reasonable time frame.
- Standardization should not compromise either the privacy or FAR of PPBSs.
- Certain tools and mechanisms in PPBSs are unique, thus it is challenging to have a generalized standardized framework.

V. CHALLENGES AND FUTURE DIRECTIONS OF PPBSs

Although some PPBSs have been proposed in recent years, the research on PPBSs is still far from mature, alongside with many open issues and challenges. All these should be addressed before PPBSs can take over the traditional verification schemes in real world applications. In this section, we will discuss some of the major challenges and future research directions of PPBSs.

- *Optimum PPBS selection:* It is extremely difficult, if not impossible, to develop a PPBS which can satisfy all performance requirements, such as low FRR, FAR, privacy leakage and computational complexity. However, depending on the application scenario, some of the requirements are more crucial than the others. So, it is important to develop a generalized framework to find the optimum privacy-preserving scheme for a given application scenario. This can be implemented by developing a weighted cost (or objective) function which utilizes the objective measures of the requirements.
- *Alignment of biometric features:* The performance of PPBSs relies on the alignment of biometric features in one way or the other. As we have discussed, in PPBSs, the original biometric feature set is discarded and only the altered biometric feature set, known as helper data, is stored. In some cases, it is difficult to successfully verify the received biometric signal from the stored helper data alone and some extra information should be used to ensure alignment. Enbo *et al.* proposed a fuzzy vault mechanism based on geometric hashing for fingerprint feature alignment [91] but it has high FRR. To deal with the problem of biometric feature misalignment, one needs to either ensure alignment in the transformed domain or make system matching performance independent of alignment. A potential solution to this is to exploit the transforms which were used to resist geometric attacks in image watermarking.
- *Utilization of unconventional biometric traits:* Nowadays, more and more people are using various interactive interfaces for various purposes, ranging from using touch-screen based smart phone/notebooks to using motion sensor based gaming devices. To facilitate these new applications, there are demands to develop novel PPBSs which could employ unconventional biometric traits such as palmprint, keystroke dynamics and body-movement-pattern [1]. When selecting new biometric traits, factors such as permanence, measurability, uniqueness and reliability should be considered.
- *Attack tolerance and analysis of accuracy:* We have discussed several common attacks on PPBSs but there is no doubt that new attacks will emerge in future applications. New methods which can resist these attacks need to be developed and evaluated. Moreover, some objective measures should be proposed to quantify the severity of the attacks. This will aid in adjusting the parameters of PPBSs according to the robustness requirement of the intended application.
- *Standardization of performance metrics:* When implementing PPBSs in large scale, compatibility between different schemes and modules can become a very challenging issue. Unified standards are needed in the development of such systems to guarantee interoperability. Some preliminary work on standardization has been

reported in the literature such as in [90] but much more needs to be done.

- *Novel privacy-preserving techniques:* Some privacy preserving methods have been proposed for PPBSs, such as fuzzy vault and biohashing. However, they failed to satisfy some important requirements, e.g., low privacy leakage and low computational complexity. Hence, novel privacy-preserving techniques should be invented to protect the privacy of the stored biometric data. This could be investigated from different aspects. For example, digital watermarking techniques can be used to protect the privacy of biometric features by hiding them into a cover multimedia object. Besides, since digital watermarking techniques can correctly extract the hidden biometric features using a secret key, even under attacks, they can also provide high level of verification accuracy.
- *Extension of privacy-preserving biometrics to other applications:* One of such extensions can be the security of the stored private data on cloud. For instance, the key generated in biometric encryption can be used to encrypt and decrypt the data before storing and retrieving it on the cloud. Privacy preserving biometrics can also be used in applications like e-business, where information is a vital asset and must be kept in a trusted environment and efficiently managed only by authorized parties. The main challenge is to develop a framework which ensures data exchanging in a secure manner.
- *Adjustable PPBSs:* In the near future, most software will have at least two different versions: mobile version and cloud version. The mobile version should have attributes such as low computational complexity and low storage requirement while the cloud version should provide exceptional verification performance and high robustness against attacks. Hence, the future PPBSs should be flexible in a way that its characteristics should be adjustable according to the necessity of the application.

VI. CONCLUSION

Privacy preservation in biometric based verification systems is a growing area of research with many challenges. This paper first outlined the basic framework and performance measures of PPBSs. Then it provided a comprehensive review of the existing PPBSs, including biometric encryption based schemes, cancelable biometric based schemes, multimodal and hybrid based schemes, and SC based schemes. The problems associated with the existing PPBSs were also summarized and discussed. Furthermore, we highlighted the challenges and future directions of PPBSs. It is hoped that the review and analysis presented in this paper can help and motivate researchers to develop more effective and efficient PPBSs in the future.

REFERENCES

[1] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*. New York, NY, USA: Springer, 2008.

[2] A. Cavoukian and A. Stoianov, "Biometric encryption," *Encyclopedia of Cryptography and Security*. New York, NY, USA: Springer, 2009.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, Apr. 2001.

[4] R. Belguechi, E. Cherrier, V. Alimi, P. Lacharme, and C. Rosenberger, *An Overview on Privacy Preserving Biometrics*. Rijeka, Croatia: InTech, 2011.

[5] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics,"*EURASIP J. Inf. Secur.*, p. 3, Sep. 2011.

[6] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure biometrics: Concepts, authentication architectures and challenges," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 51–64, Sep. 2013.

[7] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, Sep. 2015.

[8] C. Rathgeb and C. Busch, *Multi-Biometric Template Protection: Issues and Challenges*. Rijeka, Croatia: InTech, 2012.

[9] J. Bringer, H. Chabanne, and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation: An overview and recent trends," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 42–52, Mar. 2013.

[10] H. S. G. Pussewalage, J. Hu, and J. Pieprzyk, "A survey: Error control methods used in bio-cryptography," in *Proc. 10th Int. Conf. Natural Comput.*, Aug. 2014, pp. 956–962.

[11] B. Biggio, G. Fumera, P. Russu, L. Didaci, and F. Roli, "Adversarial biometric recognition: A review on biometric system security from the adversarial machine-learning perspective," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 31–41, Sep. 2015.

[12] M. Lim, A.-B. Teoh, and J. Kim, "Biometric feature-type transformation: Making templates compatible for secret protection," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 77–87, Sep. 2015.

[13] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics systems under spoofing attack: An evaluation methodology and lessons learned," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 20–30, Sep. 2015.

[14] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 54–65, Sep. 2015.

[15] M. Barni, G. Droandi, and R. Lazzeretti, "Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 66–76, Sep. 2015.

[16] Y. Wang, S. Rane, S. C. Draper, and P. Ishwar, "A theoretical analysis of authentication, privacy, and reusability across secure biometric systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1825–1840, Dec. 2012.

[17] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. EUROCRYPT*, 2004, pp. 523–540.

[18] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[19] C. Soutar, G. J. Tomko, and G. J. Schmidt, "Fingerprint controlled public key cryptographic system," U.S. Patent 5 541 994, Jul. 30, 1996.

[20] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2002, p. 408.

[21] T. C. Clancy, N. Kiyavash, and D. L. Lin, "Secure smartcard based fingerprint authentication," in *Proc. ACM SIGMM Workshop Biometrics Methods Appl.*, 2003, pp. 45–52.

[22] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744–757, Dec. 2007.

[23] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, and J. Tian, "An alignment-free fingerprint cryptosystem based on fuzzy vault scheme," *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 207–220, 2010.

[24] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *Proc. IEEE 19th Int. Conf. Pattern Recognit.*, Dec. 2008, pp. 1–4.

[25] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Improved chaff point generation for vault scheme in bio-cryptosystems," *IET Biometrics*, vol. 2, no. 2, pp. 48–55, Jun. 2013.

[26] X. Wu, N. Qi, K. Wang, and D. Zhang, "A novel cryptosystem based on iris key generation," in *Proc. 4th Int. Conf. Natural Comput.*, 2008, pp. 53–56.

[27] X. Wu, K. Wang, and D. Zhang, "A cryptosystem based on palmprint feature," in *Proc. 19th Int. Conf. Pattern Recognit.*, 2008, pp. 1–4.

[28] Y. Wu and B. Qiu, "Transforming a pattern identifier into biometric key generators," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2010, pp. 78–82.

[29] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. Comput. Commun. Secur.*, 1999, pp. 28–36.

[30] J. Bringer, H. Chabanne, G. Cohen, and B. Kindarji, "Theoretical and practical boundaries of binary secure sketches," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 673–683, Dec. 2008.

[31] C. Rathgeb and A. Uhl, "Context-based texture analysis for secure revocable iris-biometric key generation," in *Proc. 3rd Int. Conf. Imag. Crime Detect. Prevent.*, 2009, pp. 1–6.

[32] A. Teoh and J. Kim, "Secure biometric template protection in fuzzy commitment scheme," *IEICE Electron. Exp.*, vol. 4, no. 23, pp. 724–730, Dec. 2007.

[33] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in *Proc. IEEE Workshop Inf. Forensics Secur.*, Dec. 2010, pp. 1–6.

[34] M. van der Veen, T. Kevenaar, G. J. Schrijen, T. H. Akkermans, and F. Zuo, "Face biometrics with renewable templates," *Proc. SPIE*, pp. 205–216, Feb. 2006.

[35] E. Maiorana and P. Campisi, "Fuzzy commitment for function based signature template protection," *IEEE Signal Process. Lett.*, vol. 17, no. 3, pp. 249–252, Mar. 2010.

[36] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, Jan. 2008, Art. no. 113.

[37] Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jun. 2004, pp. 2203–2206.

[38] T. Scheidat, C. Vielhauer, and J. Dittmann, "An iris-based interval-mapping scheme for biometric key generation," in *Proc. 6th Int. Symp. Image Signal Process. Anal.*, 2009, pp. 511–516.

[39] S. Hoque, M. Fairhurst, and G. Howells, "Evaluating biometric encryption key generation using handwritten signatures," in *Proc. IEEE Symp. Bio-Inspired Learn. Intell. Syst. Secur.*, Aug. 2008, pp. 17–22.

[40] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," in *Proc. 7th Workshop Multimedia Secur.*, 2005, pp. 111–116.

[41] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, 2004, pp. 82–91.

[42] M. Blanton and M. Aliasgari, "Analysis of reusability of secure sketches and fuzzy extractors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 9, pp. 1433–1445, Sep. 2013.

[43] W. Yang, J. Hu, and S. Wang, "A delaunay triangle-based fuzzy extractor for fingerprint authentication," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 66–70.

[44] Q. Li, M. Guo, and E.-C. Chang, "Fuzzy extractors for asymmetric biometric representations," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2008, pp. 1–6.

[45] A. T. B. Jin, D. N. C. Ling, and A. Goh, "BioHashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, Apr. 2004.

[46] T. Connie, A. Teoh, M. Goh, and D. Ngo, "PalmHashing: A novel approach for dual-factor authentication," *Pattern Anal. Appl.*, vol. 7, no. 3, pp. 255–268, Aug. 2004.

[47] S. C. Chong, A. B. J. Teoh, and D. C. L. Ngo, "Iris authentication using privatized advanced correlation filter," in *Proc. Int. Conf. Biometrics*, 2006, pp. 382–388.

[48] A. B. J. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on BioHash," *Pattern Recognit.*, vol. 41, no. 6, pp. 2034–2044, 2008.

[49] L. Nanni and A. Lumini, "Empirical tests on BioHashing," *Neurocomputing*, vol. 69, nos. 16–18, pp. 2390–2395, Oct. 2006.

[50] R. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognit.*, vol. 40, no. 3, pp. 1057–1065, Mar. 2007.

[51] L. Nanni and A. Lumini, "Local binary patterns for a hybrid fingerprint matcher," *Pattern Recognit.*, vol. 41, no. 11, pp. 3461–3466, Nov. 2008.

[52] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[53] S. G. Kanade, D. Petrovska-Delacrétaz, and B. Dorizzi, *Enhancing Information Security and Privacy: Combining Biometrics & Cryptography* (Synthesis Lectures on Information Security, Privacy, and Trust). New York, NY, USA: Morgan & Claypool Publishers, 2012.

[54] Q. Feng, F. Su, A. Cai, and F. Zhao, "Cracking cancelable fingerprint template of Ratha," in *Proc. Int. Symp. Comput. Sci. Comput. Technol.*, 2008, pp. 572–575.

[55] A. B. J. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 37, no. 5, pp. 1096–1106, Oct. 2007.

[56] Y. Wang and D. Hatzinakos, "On random transformations for changeable face verification," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 41, no. 3, pp. 840–854, Jun. 2011.

[57] C. Rathgeb, F. Breitinger, and C. Busch, "Alignment-free cancelable iris biometric templates based on adaptive bloom filters," in *Proc. IEEE Int. Conf. Biometrics*, Jun. 2013, pp. 1–8.

[58] P. P. Paul and M. Gavrilova, "Multimodal cancelable biometrics," in *Proc. IEEE 11th Int. Conf. Cognit. Inform. Cognit. Comput.*, Aug. 2012, pp. 43–49.

[59] S. Vasuhi, V. Vaidehi, N. T. N. Babu, and T. M. Treesa, "An efficient multimodal biometric person authentication system using fuzzy logic," in *Proc. IEEE Int. Conf. Adv. Comput.*, Dec. 2010, pp. 74–81.

[60] S. Awang, R. Yusof, M. F. Zamzuri, and R. Arfa, "Feature level fusion of face and signature using a modified feature selection technique," in *Proc. Int. Conf. Signal-Image Technol. Internet-Based Syst.*, 2013, pp. 706–713.

[61] M. F. Nadheen and S. Poornima, "Fusion in multimodal biometric using iris and ear," in *Proc. IEEE Int. Conf. Inf. Commun. Technol.*, Apr. 2013, pp. 83–87.

[62] P. P. Paul and M. Gavrilova, "Rank level fusion of multimodal cancelable biometrics," in *Proc. IEEE 13th Int. Conf. Cognit. Inform. Cognit. Comput.*, Aug. 2014, pp. 80–87.

[63] L. Yuan, "Multimodal cryptosystem based on fuzzy commitment," in *Proc. IEEE 17th Int. Conf. Comput. Sci. Eng.*, Dec. 2014, pp. 1545–1549.

[64] J. Bringer, H. Chabanne, and B. Kindarji, "The best of both worlds: Applying secure sketches to cancelable biometrics," *Sci. Comput. Program.*, vol. 74, nos. 1–2, pp. 43–51, Dec. 2008.

[65] W. J. Wong, M. L. D. Wong, and A. B. J. Teoh, "A security- and privacy-driven hybrid biometric template protection technique," in *Proc. Int. Conf. Electron., Inf. Commun.*, 2014, pp. 1–5.

[66] M. M. Monwar and M. L. Gavrilova, "Enhancing security through a hybrid multibiometric system," in *Proc. IEEE Int. Conf. Comput. Intell. Biometrics, Theory, Algorithms, Appl.*, Mar./Apr. 2009, pp. 84–91.

[67] H.-H. Zhu, Q.-H. He, and Y.-X. Li, "A two -step hybrid approach for voiceprint-biometric template protection," in *Proc. IEEE Int. Conf. Mach. Learn.*, Jul. 2012, pp. 560–565.

[68] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, 1978.

[69] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, 2009, pp. 169–178.

[70] C. Gentry and S. Halevi, "Implementing Gentry's fully-homomorphic encryption scheme," in *Proc. 30th Annu. Int. Conf. EUROCRYPT*, 2011, pp. 129–148.

[71] T. Plantard, W. Susilo, and Z. Zhang, "Fully homomorphic encryption using hidden ideal lattice," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2127–2137, Dec. 2013.

[72] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. EUROCRYPT*, 1999, pp. 223–238.

[73] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich, "SCiFI—A system for secure face identification," in *Proc. IEEE Int. Conf. Secur. Privacy*, May 2010, pp. 239–254.

[74] M. O. Rabin, "How to exchange secrets with oblivious transfer," Aiken Comput. Lab, Harvard Univ., Cambridge, MA, USA, Tech. Rep. TR-81, 1981.

[75] A. C.-C. Yao, "How to generate and exchange secrets (extended abstract)," in *Proc. 27th Annu. Symp. Found. Comput. Sci.*, 1986, pp. 162–167.

[76] M. Blanton and P. Gasti, "Secure and efficient protocols for iris and fingerprint identification," in *Proc. 16th Eur. Conf. Res. Comput. Secur.*, 2011, pp. 190–209.

[77] H. Chun, Y. Elmehdwi, F. Li, P. Bhattacharya, and W. Jiang, "Outsourceable two-party privacy-preserving biometric authentication," in *Proc. 9th ACM Symp. Inf., Comput. Commun. Secur.*, 2014, pp. 401–412.

[78] P. Bogetoft *et al.*, "Secure multiparty computation goes live," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science). New York, NY, USA: Springer, 2009, pp. 325–343.

[79] K. Simoens, J. Bringer, H. Chabanne, and S. Seys, "A framework for analyzing template security and privacy in biometric authentication systems," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 833–841, Apr. 2012.

[80] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Proc. IEEE Int. Conf. Biometrics*, Sep. 2007, pp. 1–6.

[81] A. Adler, "Reconstruction of source images from quantized biometric match score data," in *Proc. Int. Conf. Biometrics*, Sep. 2004, pp. 43–98.

[82] P. Mihăilescu, A. Munk, and B. Tams, "The fuzzy vault for fingerprints is vulnerable to brute force attack," in *Proc. BIOSIG*, vol. 155. 2009, pp. 43–54.

[83] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—Part II: Multiple use case," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 140–151, Mar. 2011.

[84] J. Bringer, H. Chabanne, and C. Morel, "Shuffling is not sufficient: Security analysis of cancelable iriscodes based on a secret permutation," in *Proc. IEEE Int. Conf. Biometrics*, Sep./Oct. 2014, pp. 1–8.

[85] A. Nagar and A. K. Jain, "On the security of non-invertible fingerprint template transforms," in *Proc. 1st IEEE Int. Workshop Inf. Forensics Secur.*, Dec. 2009, pp. 81–85.

[86] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[87] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography—Part II: CR capacity," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 225–240, Jan. 1998.

[88] *JTC1 SC27 IT Security Techniques: Biometric Information Protection*, document ISO/IEC 24745, Intl Organization for Standardization, 2011.

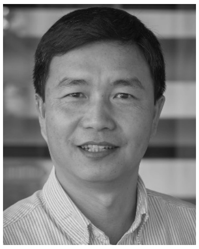
[89] *JTC1 SC37 Biometrics, Parts 1-7: Biometric Performance Testing and Reporting*, document ISO/IEC 19795, Intl Organization for Standardization, 2012.

[90] *Performance Testing of Biometric Template Protection Schemes*, document WD 30136, ISO/IEC working draft, 2014.

[91] F. Enbo, H. Caiyun, and L. Jiayong, "Auto-aligned sharing fuzzy fingerprint vault," *China Commun.*, vol. 10, no. 10, pp. 145–154, Oct. 2013.

IYNKARAN NATGUNANATHAN received the B.Sc.Eng. (Hons.) degree in electronics and telecommunication engineering from the University of Moratuwa, Katubedda, Sri Lanka, in 2007, and the Ph.D. degree from Deakin University, VIC, Australia, in 2012. From 2006 to 2008, he was a Software Engineer with Millennium Information Technology (Pvt) Ltd., Malabe, Sri Lanka. He is currently a Research Fellow with the School of Information Technology, Deakin University. His research interests include digital watermarking, audio and image processing, telecommunication, and robotics.

ABID MEHMOOD received the bachelor's degree in computer science from the COMSATS Institute of Information Technology, Pakistan, in 2006, and the master's degree in information technology from the University of Ballarat, Australia, in 2009. He is currently pursuing the Ph.D. degree with Deakin University, Australia.



YONG XIANG (SM'12) received the Ph.D. degree in electrical and electronic engineering from The University of Melbourne, Australia. He is currently a Professor and the Director of the Artificial Intelligence and Image Processing Research Cluster with the School of Information Technology, Deakin University, Australia. He has authored over 110 refereed journal and conference papers. His research interests include information security and privacy, multimedia (speech/image/video) processing, wireless sensor networks, massive MIMO, and biomedical signal processing. He is an Associate Editor of the IEEE Signal Processing Letters and IEEE Access. He has served as the Program Chair, TPC Chair, Symposium Chair, and Session Chair for a number of international conferences.

GLEB BELIAKOV (M'08–SM'08) received the Ph.D. degree in physics and mathematics from Peoples' Friendship University, Moscow, Russia, in 1992. He was a Lecturer and a Research Fellow with Los Andes University and the Universities of Melbourne and South Australia. He is currently a Professor with the School of Information Technology, Deakin University, Australia. His research interests include aggregation operators, multivariate approximation, global optimization, and decision support systems. He has authored over 150 research papers and a monograph in the mentioned areas, and a number of software packages. He serves as an Associate Editor of the IEEE Transactions on Fuzzy Systems, and the journals *Fuzzy Sets and Systems* and *TOP*.

JOHN YEARWOOD received the B.Sc. degree from Monash University, Australia, the M.Sc. degree from Sydney University, Australia, and the Ph.D. degree from RMIT University, Australia. In 1989, he was a Lecturer with the School of Information Technology and Mathematical Science, University of Ballarat, Australia, where he was appointed as a Professor in 2007. He is currently a Professor and the Head with the School of Information Technology, Deakin University, Australia. He has authored over 140 refereed journals, book chapters, and conference articles. His research interest includes modern optimization theory and techniques and their applications in pattern recognition, signal processing, and decision support systems.