Pattern Recognition 56 (2016) 50–62

Contents lists available at ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation

Zhe Jin [a], Andrew Beng Jin Teoh [b,*], Bok-Min Goi [a], Yong-Haur Tay [a]

[a] Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman, Kuala Lumpur, Malaysia
[b] School of Electrical and Electronic Engineering, College of Engineering, Yonsei University, Seoul, South Korea

ARTICLE INFO

Article history:
Received 6 July 2015
Received in revised form
20 December 2015
Accepted 26 February 2016
Available online 8 March 2016

Keywords:
Fingerprint key binding
Cancellable templates
Error correction code free key binding
Alignment-free matching
Security–performance tradeoff

ABSTRACT

Despite fuzzy commitment (FC) is a theoretically sound biometric-key binding scheme, it relies on error correction code (ECC) completely to mitigate biometric intra-user variations. Accordingly, FC suffers from the security–performance tradeoff. That is, the larger key size/higher security always trades with poor key release success rate and vice versa. Additionally, the FC is highly susceptible to a number of security and privacy attacks. Furthermore, the best achievable accuracy performance of FC is constrained by the simple distance metrics such as Hamming distance to measure the dissimilarity of binary biometric features. This implies many efficient matching algorithms are to be abandoned. In this paper, we propose an ECC-free key binding scheme along with cancellable transforms for minutiae-based fingerprint biometrics. Apart from that, the minutiae information is favorably protected by a strong non-invertible cancellable transform, which is crucial to prevent a number of security and privacy attacks. The scheme is not limited to binary biometrics as demanded in FC but instead can be applied to various types of biometric features and hence a more effective matcher can be chosen. Experiments conducted on FVC2002 and FVC2004 show that the accuracy performance is comparable to state-of-the-arts. We further demonstrate that the proposed scheme is robust against several major security and privacy attacks.

1. Introduction

Biometric technology is likely to provide a heightened security level for identity verification and identification. Yet, the invasion of identity privacy is inevitable if the stored template is compromised. On the other hand, in cryptography, key management is mandatory for key storage, exchange and transaction, which remains a challenge task [1]. The idea of using biometrics to bind and release a cryptography key is thus attractive since biometric trait is admissibly unique [2]. In fact, the study of binding biometrics with cryptography key has been carried out in the past decade as a plausible solution for key management as well as for biometric template protection [3,4]. As a result, biometric cryptosystem was put forward to respond to the needs of either generating cryptographic key directly from biometrics (key generation) or securing the external cryptographic key using biometrics (key binding) [5]. The major distinction of key generation and key binding is on how the *helper data* (a piece of public information derived from biometrics but reveals no significant information about the original biometric data) is extracted. For key generation, the helper data is derived *solely* from the biometric template and the key is *directly* generated from the helper data and the query biometric features. Despite key generation is an attractive proposition, it is difficult to be realized due to large intra-user variability of biometrics that leads to a contradiction for achieving high key entropy and stability simultaneously [5]. Furthermore, the original idea of key generation scheme is not catered for cancelability and linkability concerns. The representative instances of key generation schemes can be found in [6–8]. It is noted that due to the nature of biometric variability, key generation is less popular than that of the key binding scheme.

For key binding approach, the chief idea is to secure the biometric template by binding it with the cryptographic key. The mixture of biometric template and key is stored as helper data [5]. The cryptographic key is externally generated and completely independent to the biometrics. A key is released only if the query instance with sufficient similarity to the template is supplied. Error correction code (ECC) is employed to manage the variations of biometric data. The well-known instances of key binding approach are fuzzy commitment [3] and fuzzy vault [4]. Despite effective, several vulnerabilities and drawbacks were recognized. This hinders the proliferation of key binding schemes. The details will be discussed in Section 1.1.

[*] Corresponding author. Tel.: +82 2 2123 5772.
E-mail address: bjteoh@ieee.org (A.B.J. Teoh).

http://dx.doi.org/10.1016/j.patcog.2016.02.024
0031-3203/© 2016 Elsevier Ltd. All rights reserved.

On the other hand, cancellable biometrics [9] is a method for biometric template protection. It refers to the irreversible transform of the biometric data to ensure security and privacy of the biometric template can be protected. Hence, instead of the original biometric data, the transformed templates are stored. If a cancellable biometric template is compromised, a new template can be regenerated from the original biometric data.

In a nutshell, while both biometric cryptosystems and cancellable biometrics serve to protect biometric template, the former is also meant to protect key in cryptographic applications. However, both approaches fall short in terms of accuracy performance, security and privacy. In this paper, a new biometric key binding scheme is proposed by bridging the biometric cryptosystem and cancellable biometrics. In some sense, our scheme achieves a middle-ground between the two main approaches but overcoming the limitations of both. It can thus be better served for both cryptographic key and biometric template protection.

The organization of this paper is as follow: in Section 1.1, we briefly describe previous work related to the key binding schemes and cancellable fingerprint template. Motivation and contribution are given in Section 1.2. Our proposed key binding scheme and its implementation are presented in Sections 2 and 3 respectively. The experimental results, security and privacy analysis are provided in Sections 4 and 5 respectively. Finally, conclusion is drawn in Section 6.

1.1. Related work

1.1.1. Fuzzy commitment

Fuzzy commitment [3] is originally designed to protect a cryptographic key and it is later being perceived as a technique for biometric template protection. Fuzzy commitment is meant to accept input in binary string form (e.g. Iriscode [58]). Assume that the enrolled biometric template b^e is a n-bits binary string, in the enrollment stage (key binding), a codeword c is generated from the cryptographic key k_c of length l $(l<n)$ with ECC. Zero padding on b^e is inevitable to ensure that both c and b^e are identical in length; then c is bit-wise XORed with b^e and renders helper data $y_c = c \oplus b^e$. The y_c is stored in the database along with $\mathbf{h}(k_c)$, where $\mathbf{h}(.)$ is a hash function. In key release stage, the query biometrics b^q is XORed with y_c to produce a corrupted codeword, $c^* = y_c \oplus b^q = c \oplus (b^e \oplus b^q)$. The c^* can be decoded to k^*, if the query bit-string is sustainably similar to the enrolled template within the capacity of the ECC. The authentication is deemed successful if $\mathbf{h}(k_c) = \mathbf{h}(k^*)$.

It has been pointed out that fuzzy commitment is *information-theoretical* secure only if the bits extracted from biometric features are uniformly and independently distributed [11]. Yet, it is not easy to achieve this requirement in practice as biometric data are inherently structured and thus the features remain correlated after going through feature extractor [11]. This will propagate to the binary representation if the binarization process is not carefully attended. Besides that, privacy leakage is another concern of fuzzy commitment due to bits redundancy introduced by ECCs [11,44,45]. The aforementioned pitfalls trigger various attacks such as decodability attack [46,47], statistical attack [48] and attack based on entropy analysis [11].

Simoen et al. [46] proposed a decodability attack against fuzzy commitment scheme that exploits the correlation of multiple helper data that generate from the same subject biometric data. Kelkboom et al. [47] further analyzed the attack and proposed a bit-permutation mechanism against decodability attack. Assume that biometric features b_1^e, b_2^e are the two references of the same subject across two different applications; c_1 and c_2 are the corresponding codewords. The helper data is obtained as $W_1^e = b_1^e \oplus c_1$ and $W_2^e = b_2^e \oplus c_2$. The attacker can perform $W_1^e \oplus W_2^e = (b_1^e \oplus b_2^e) \oplus (c_1 \oplus c_2) = (b_1^e \oplus b_2^e) \oplus c_3$. Such attack is initiated by the work of Carter and Stoianov [54] with the purpose of checking whether decoding of two helper data leads to a valid codeword. If positive, the two helper data are most likely derived from the same user. So, if $b_1^e \oplus b_2^e$ is small (this is usually true if b_1^e, b_2^e are the instances of the same user), the result of XOR operation will be close to valid codeword. $W_1^e \oplus W_2^e$ is then decodable with high probability. This attack is also known as attacks via record multiplicity (ARM), where specifically outlined by [13] for fuzzy vault.

Rathgeb et al. [48] proposed a statistical attack based on ECCs that is commonly applied in fuzzy commitment to retrieve the most likely codeword. The attacker collects adequate imposter templates b_p and performs XOR successively with the stored helper data, $s = b_e \oplus c$ where b_e is the enrolled template and c is codeword, i.e. $b_p \oplus s$. Note that b_e is segmented into multiple chunks due to the computation speed. The XOR operation is thus on chunk-basis. Thereafter, the codeword of each chunk are collected and a histogram is generated by counting the occurrence frequency of codewords. A bin of histogram corresponding to the histogram maximum is considered as a success, which yields the most likely codeword for this chunk.

Zhou et al. [11] analyzed the security and privacy leakage of fuzzy commitment thoroughly under the conditions whereby the practical biometric data are not uniformly and independently distributed. To assess the security and privacy leakage, several evaluation metrics have been proposed: 1) the security can be measured by *average min-entropy*, *conditional entropy* and *conditional guessing entropy*; 2) privacy protection consists of irreversibility and privacy leakage. Irreversibility can be measured by the same metrics in security assessment while privacy leakage can be measured by *entropy loss* and *mutual information*. With these assessment metrics, [11] concludes that the fuzzy commitment is highly vulnerable on the security and privacy leakage due to the dependency of biometric features.

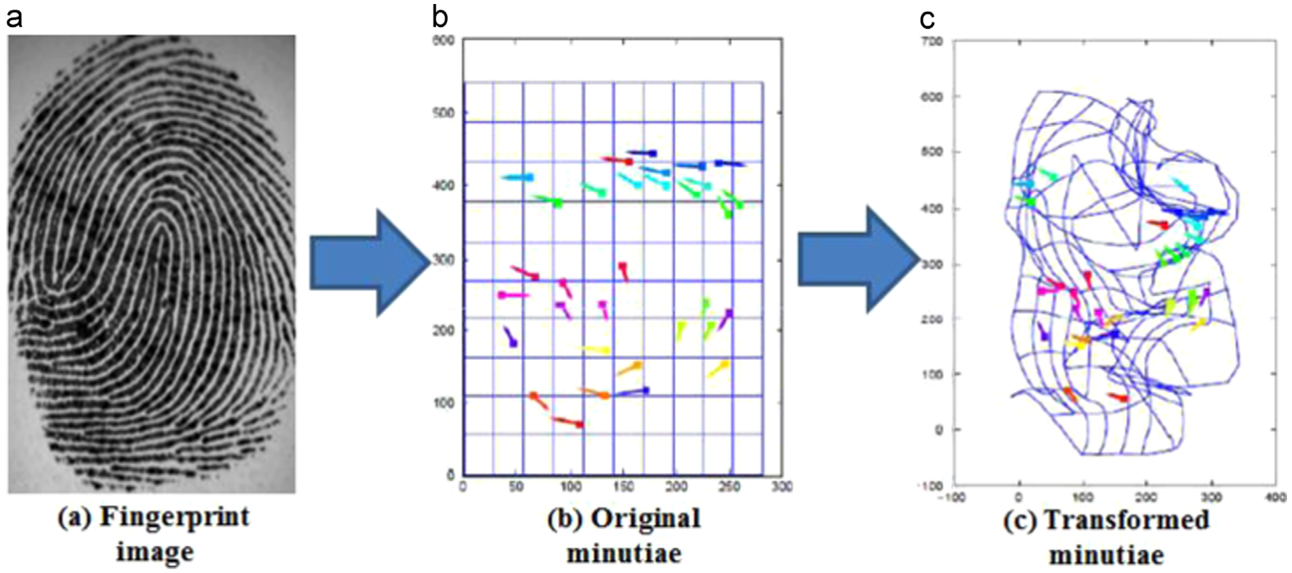
Moreover, Scheirer and Boult [13] introduced an attack, namely Surreptitious Key-Inversion Attack (SKI) on fuzzy vault, which is also an equivalently effective attack against fuzzy commitment. SKI refers to if the cryptographic key is known by an attacker, the biometric string that blends with codeword can be easily recovered through the XOR operation using the compromised cryptographic key and the secure sketch. Thus, the privacy leakage is inevitable.

Apart from that, fuzzy commitment suffers from the limitations that are associated with ECCs. Firstly, Nagar [10] and Kelkboom et al. [55] pointed out that fuzzy commitments suffers from security (key size) – performance (Genuine Acceptance Rate, GAR) tradeoff; i.e. the longer key size (higher security) results lower GAR and vice versa. In fuzzy commitments, a codeword is composed of key and redundant bits and it is known that the number of redundant bits is proportional to the error correction capacity. Therefore, the small number of redundant bits, which implies weaker correction capacity, will lead to the larger key size, which means better security. This is attributed to the requirement that the codeword size has to be matched to the size of biometric string. Secondly, Bringer et al. [14] shows that the maximum key length and the decoding accuracy are upper bounded by the error correction capacity of the chosen ECC.

Another drawback is since fuzzy commitment operates in hamming domain, it has essentially imposed a strict requirement on both biometric feature representation (i.e. binary biometrics only is allowed) and matcher (i.e. Hamming distance) [8]. This may severely limit the best achievable accuracy performance as many effective feature extractors and matchers are to be abandoned.

From the afore-discussed issues, we made the following observations:

1) Inherent dependency of biometric features. Without considering such a constraint, deployment of fuzzy commitment will



(a) Fingerprint image

(b) Original minutiae

(c) Transformed minutiae

Fig. 1. The idea of fingerprint minutia protection using many-to-one transform adopted from [9].

lead to a significant security reduction and severe privacy leakage.

2) Potentially poor accuracy performance due to the requirements of binary representation and matcher.
3) Vulnerabilities associated to ECCs such as performance-key size tradeoff and statistical attack.
4) Privacy attacks such as Decodability attack (ARM) and SKI attack.

1.1.2. Cancellable biometrics

Cancellable biometrics is truly meant designed for biometric template protection. The schemes vary according to different biometric modality but we solely focus on minutia oriented fingerprint templates. Protection of minutia template is of urgent need after Hill [23] demonstrated the first template inversion technique to recover the fingerprint minutiae. A typical method for minutia protection is by mapping two or more minutia to the same point in the transformed domain via a many-to-one transformation function as shown in Fig. 1. Therefore, it is hard to determine the original location to which a minutia belongs.

In general, minutia is the most widely used features for representing a fingerprint for recognition [56]. This is attributed to the reliability and robustness of minutiae against elastic deformation of fingerprint image. Unlike global feature such as singular point or coarse ridge line shape, minutiae provide sufficient distinctiveness for accurate matching [56]. Minutiae representation is unordered and variable in size due to the variety in terms of the numbers of spurious and missing genuine minutiae occurred in multiple impressions of the same finger.

Minutiae-based fingerprint template protection techniques can be divided into two categories: fixed-length representation and variable size representation. For the former, it refers to the fingerprint template that is fixed in size, such as in a feature (or binary) vector form in length n, which primarily can serve biometric cryptosystems, e.g. fuzzy commitment; while if the representation is of variable in size, it falls into the latter category, which is more suitable for cancellable biometrics. A variable size representation can be represented in a matrix form with size $m \times n$, where m is determined by the number of minutiae extracted from a fingerprint image and n is the length of the feature vector that derived from a single minutia.

In fixed-length template approach, Farooq et al. [24] generated a binary fingerprint representation based on the histograms of triangular features generated from minutiae triplets. Seven invariant features: length of three sides, three angles between each side and each minutia orientation; and height of the triangle are extracted and quantized into 24 bits, which yields a 2^{24} bit binary string. Revocability is achieved by permuting the binary string using external seed. However, this method requires high computational cost due to the exhaustive calculation of features for all possible minutiae triplets. Following this work, Jin et al. [25] attempted to reduce the length of bit-string by using minutiae pairs instead of minutiae triplets. Consequently, the size of template is reduced to 2^{18} and the performance is enhanced using a majority-voting-based training process.

Xu et al. [26] proposed a Spectral Minutiae approach to convert a set of minutiae into a fixed-length feature vector. The proposed approach performs Fourier transform on a minutia set and remaps the Fourier spectral magnitude onto polar-logarithmic coordinate. An analytical representation for minutiae is further proposed to minimize error, which can directly be evaluated on polar-logarithmic grids. As the number of grids is fixed, a fixed-length representation can be derived. However, the accuracy of this approach over point-to-point (minutiae) and two-stage procedure matching (minutia descriptor) approaches is inferior.

Nagar et al. [27] considered a robust set of features by considering the average minutia coordinate within a cuboid, the standard deviation of the minutiae coordinates, and the aggregate wall distance. This method offers high accuracy performance but it demands registration points (e.g. high curvature points) to align the fingerprint image prior to feature extraction. Yet, the detection of registration points can be challenging on poor-quality images.

For variable size template approach, Yang and Busch [29] proposed a fingerprint template protection method based on minutia vicinity. Given N minutiae $\{fm_i \mid i=1, 2,\ldots, N\}$, each minutia fm_i with the three nearest neighboring minutiae $\{c_{i1}, c_{i2}$ and $c_{i3}\}$ together form a set of minutia vicinity $V_i=\{fm_i, c_{i1}, c_{i2}, c_{i3} \mid i=1, 2,\ldots, N\}$. Each minutia vicinity comprises 12 orientation vectors: $m_i \rightarrow c_{i1}$, $c_{i2} \rightarrow c_{i3}$, $c_{i3} \rightarrow c_{i1,}$ etc. The four coordinate pairs of V_i are then transformed based on the 5 (out of 12) randomly selected orientation vectors in the respective minutia vicinity. Next, the random offsets are added to each V_i in order to conceal the local topological relationship among the minutiae in the vicinity. The transformed minutiae are thus regarded as a protected minutia vicinity with stored random offsets. However, Simoens et al. [30] pointed out that the coordinates and orientations of minutiae in [29] could easily be revealed if both random offsets and orientation vectors are disclosed to the adversary. They also showed that the attack complexity is considerably low (e.g., only 2^{17} attempts are required when the random offsets table is known with reference to 2^{120} attempts when the random offsets table is not known).

Ferrara et al. [31] proposed a recovery algorithm to restore the original minutiae from the minutiae cylinder-code (MCC) [32]-a state-of-the-art fingerprint template representation. A non-invertible scheme is hence proposed, namely protected minutia cylinder-code (P-MCC) via binary principle component analysis. Although the non-invertibility of P-MCC has been experimentally justified, it is still unable to fully protect the genuine minutiae points. For instance, it has been reported that a portion of genuine minutiae (at least 25.4%) could be precisely recovered [31]. Recently, a two-factor protection scheme on P-MCC, namely 2P-MCC [43] is proposed to make the P-MCC revocable.

Wang and Hu [33] proposed a scheme based on dense infinite-to-one mapping (DITOM) technique. DITOM extracts three invariant features from a pair of minutiae. The extracted features are then quantized, hashed and binarized. Lastly, a complex-valued vector is generated from the resultant bit-string by applying discrete Fourier transform and the final template is obtained by blending the complex vector with a random matrix. However, ARM is possible when multiple templates are known to adversary.

From the above literature review, we make the following observations:

(1) Some of the afore-discussed “non-invertible transforms” are in fact susceptible to partial or full inversion (e.g., [29,33]).
(2) Alignment is often required for accurate matching [27].
(3) Some methods have yet to catch up the satisfactory accuracy compare to pure minutiae matching approach [24–26,33].
(4) Some methods suffer from high computation cost and large storage for template [24,25].

Ideally, a well-designed biometric template protection scheme must satisfy the following four requirements:

- *Non-linkability*. It should be computationally hard to differentiate multiple instances of the protected biometric reference derived from the same biometric trait. Non-linkability prevents the cross-matching across different applications. Note that ARM in fuzzy commitment is indeed an attack instance that violets this criterion.
- *Cancelability*. A new template can be reissued once the old template is compromised.
- *Non-invertibility*. It should be computationally infeasible to derive the original biometric template from the protected template or/and the helper data.
- *Performance preservation*. The accuracy performance of the protected template should be preserved or improved.

1.2. Motivation and contribution

In Section 1.1, we have summarized the limitations of both biometric cryptosystems and cancellable biometrics. It is indeed challenging to resolve all these problems in their own regime. However, we believe that the assimilation of both approaches would be a plausible response to this open problem.

In this paper, we proposed an ECC-free key binding scheme along with cancellable transforms for minutiae-based fingerprint biometrics in place of fuzzy commitments. This idea is inspired from *chaffing and winnowing scheme*, which was conceived by Ron Rivest [34]. The goal of chaffing and winnowing is to achieve confidentiality without using encryption when sending data over an insecure channel. However, the scheme that often used in conventional cryptography context cannot be applied directly to biometrics due to the stochastic nature of biometric data as well as various unique design criteria as aforementioned. Therefore, a major alteration to the original scheme has to be carried out.

In our realization, we adopt our previous proposed alignment-free minutia descriptor, namely Minutia Vicinity Decomposition (MVD) [35] and a modified non-invertible transform, called Graph-based Hamming Embedding (GHE) to construct an adoptive cancellable transform that facilitates the binding of cryptographic key with fingerprint biometrics. The main contributions of this paper are as follows:

- A new ECC-free biometric key binding scheme and the realization in fingerprint biometrics are proposed. Since ECC is abandoned, the issues that associate with ECC such as security-performance tradeoff and statistical attack are no longer exist.
- A modified randomized GHE in constructing the cancellable transform is proposed. Therefore, cancelability criterion for template protection is satisfied.
- We performed several security and privacy analysis for the proposed scheme, particularly focus on the major privacy attacks, such as ARM and SKI.
- The proposed scheme is not limited to the binary feature representation and the matcher, but it can be applied to variety of biometric feature representations.

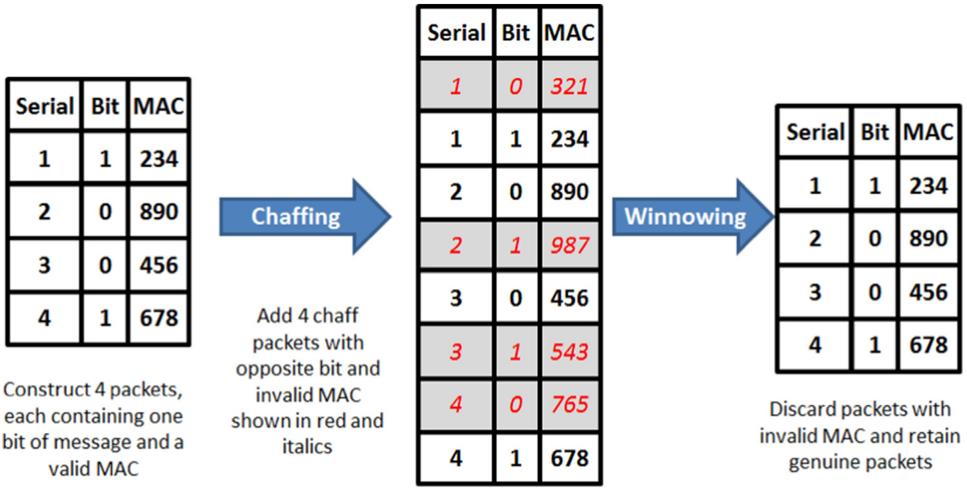
2. Proposed biometric key binding scheme

2.1. Methodology

In this section, we first review the conventional chaffing and winnowing scheme (CWS) [34], which is the primary source that inspired our work. The CWS comprises of two stages: 1) adding the fake packets (chaffs) and bogus message authentication code (MACs) based on a sequence of number and message, i.e. chaffing; 2) discarding packets with bogus MACs at receiver, i.e. winnowing. In this regard, an eavesdropper is clueless to identify which package is real or bogus without secret key information that is only shared by the genuine sender and receivers. An example of CWS is demonstrated in Fig. 2. Unfortunately, conventional CWS is not directly transferrable to the biometric-key binding scheme due to the fuzziness of biometric data as well as various unique design criteria as presented in Section 1.1.

Our proposed biometric-key binding scheme is illustrated in Fig. 3. For key binding, given a binary key k, encode 1s in k with true templates while encode 0s with synthetic templates. The encoding process is to apply cancellable transform to either true or synthetic biometric templates with *different* transformation seed, in order to produce a series of cancellable templates. One cancellable transform consists of one permutation process along with GHE as shown in Fig. 3. It is noted that for m-bits key, m cancellable transforms are required to encode the key entirely. This process corresponds to “chaffing” in CWS.

On the other hand, the key release consists of a two-steps procedure: 1) apply m cancellable transforms to the query data yield m cancellable query instances; 2) match the cancellable query instances with the stored cancellable templates and compare the matching score with respect to a pre-defined threshold τ. If the matching score $s \geq \tau$, release 1; otherwise 0. This corresponds to “winnowing” in CWS. The detailed algorithms for key binding and key release are presented in Algorithms 1 and 2 as follows. Note that the similarity function (sim(.)) in Algorithm 2 is detailed in Section 3.3. More importantly, other matchers can be flexibly replaced and integrated into the proposed key binding scheme.



Serial	Bit	MAC
1	1	234
2	0	890
3	0	456
4	1	678

Construct 4 packets, each containing one bit of message and a valid MAC

Add 4 chaff packets with opposite bit and invalid MAC shown in red and italics

Serial	Bit	MAC
1	*0*	*321*
1	1	234
2	0	890
2	*1*	*987*
3	0	456
3	*1*	*543*
4	*0*	*765*
4	1	678

Serial	Bit	MAC
1	1	234
2	0	890
3	0	456
4	1	678

Discard packets with invalid MAC and retain genuine packets

Fig. 2. An example of chaffing and winnowing scheme adopted from [57].

Algorithm 1. Key binding (Enrollment).

```
Input: True template $\mathbf{\Omega}^e$, synthetic template $\mathbf{\Omega}^s$, $m$-bits key
  $k \in 0, 1$, $m$ cancellable transforms $C_{i=1}^m$
Encode $m$-bits key $k$ using $m$ cancellable transforms
For $i = 1:m$
  if $k_i = 1$
     $\Xi_i^c = C_i(\mathbf{\Omega}^e)$
  else
     $\Xi_i^c = C_i(\mathbf{\Omega}^s)$
End for
Output: A set of cancellable templates $\Xi_{i=1...m}^c$
```

Algorithmm 2. Key extraction (Authentication).

```
Input: A set of cancellable templates $\Xi^c$ obtained in Algorithm
  1, matching threshold $\tau$, query biometric $\mathbf{\Omega}^q$, $m$ cancellable
  transforms $C_{i=1}^m$ used in Algorithm 1.
Step 1: Applying $m$ cancellable transforms on query biometric.
For $i = 1:m$
  $\Xi_i^q = C_i(\mathbf{\Omega}^q)$
End for
Step 2: Match the enrolled cancellable templates $\Xi^c$ with query
  cancellable templates $\Xi^q$ computed in step 1 and release 1 or
  0 based on similarity score. sim(.) denotes the similarity
  measure function.
For $i = 1:m$
  sim($\Xi_i^q$, $\Xi_i^c$)=$s$
    if $s \geq \tau$
       $\overline{k_i} = 1$
  else
       $\overline{k_i} = 0$
End for
Output: Released $m$-bits key $\overline{k}$.
```

2.2. Synthetic templates generation

For key binding purpose, the proposed method employs both true and synthetic templates to generate a set of cancellable templates. We suggest several options to create synthetic templates: 1) use different biometric modalities. For instance, fingerprint template for true template and palmprint template for synthetic template etc.; 2) use two different feature extraction algorithms on the same biometric data to generate true and synthetic templates; 3) use imposter template as synthetic template.

However, an inconsiderate design of synthetic templates may leads to the revelation of the cryptography key easily. For example, if the sizes of synthetic and true template differ and propagate to the cancellable template stage, the key can be easily determined. This is typical for fingerprint minutia as they are point set variable in size. Furthermore, the cancellable synthetic template should not be statistically differentiable to the cancellable true templates. For instance, the elements in a cancellable synthetic template are ranged from 0 to 1 while the range of cancellable true template is -1 to 0.

In this paper, we use randomly permuted true templates to generate the synthetic templates. These synthetic templates are: 1) of same length with true templates; 2) the randomized true templates after cancellable transform. Hence it is highly unlikely to distinguish the true templates and synthetic templates statistically. The synthetic templates generation can be expressed as follows:

$$\mathbf{\Omega}_i^s = \mathrm{Perm}\left(\mathbf{\Omega}_i^e\right) \; (i = 1, \ldots, N) \tag{1}$$

where $\mathbf{\Omega}^s$ and $\mathbf{\Omega}^e$ represent the synthetic and true templates, respectively and Perm(.) denotes the random permutation function. The permutation seed is discarded after enrollment process is completed. In our implementation, $\mathbf{\Omega}_i$ refers to the i-th row of minutiae vicinity decomposition (MVD) [35] and N is the total number of vicinities extracted from minutia set.

2.3. Cancellable templates generation

With the synthetic and true templates, the cryptography key can be encoded via a set of cancellable templates. The cancellable templates generation essentially consists of a two-steps procedure: 1) random permutation; 2) non-invertible feature transformation. The steps are described as follows:

1) ***Random permutation***. In order to bind a m-bits key, m random permutations are required to generate m cancellable templates so that each cancellable template is used to encode each bit of cryptography key. For key binding, random permutation with different seed recurs for true and synthetic templates subject to the specific bit in the key as expressed in Eq. (2), while in the key release stage, random permutation is applied to query

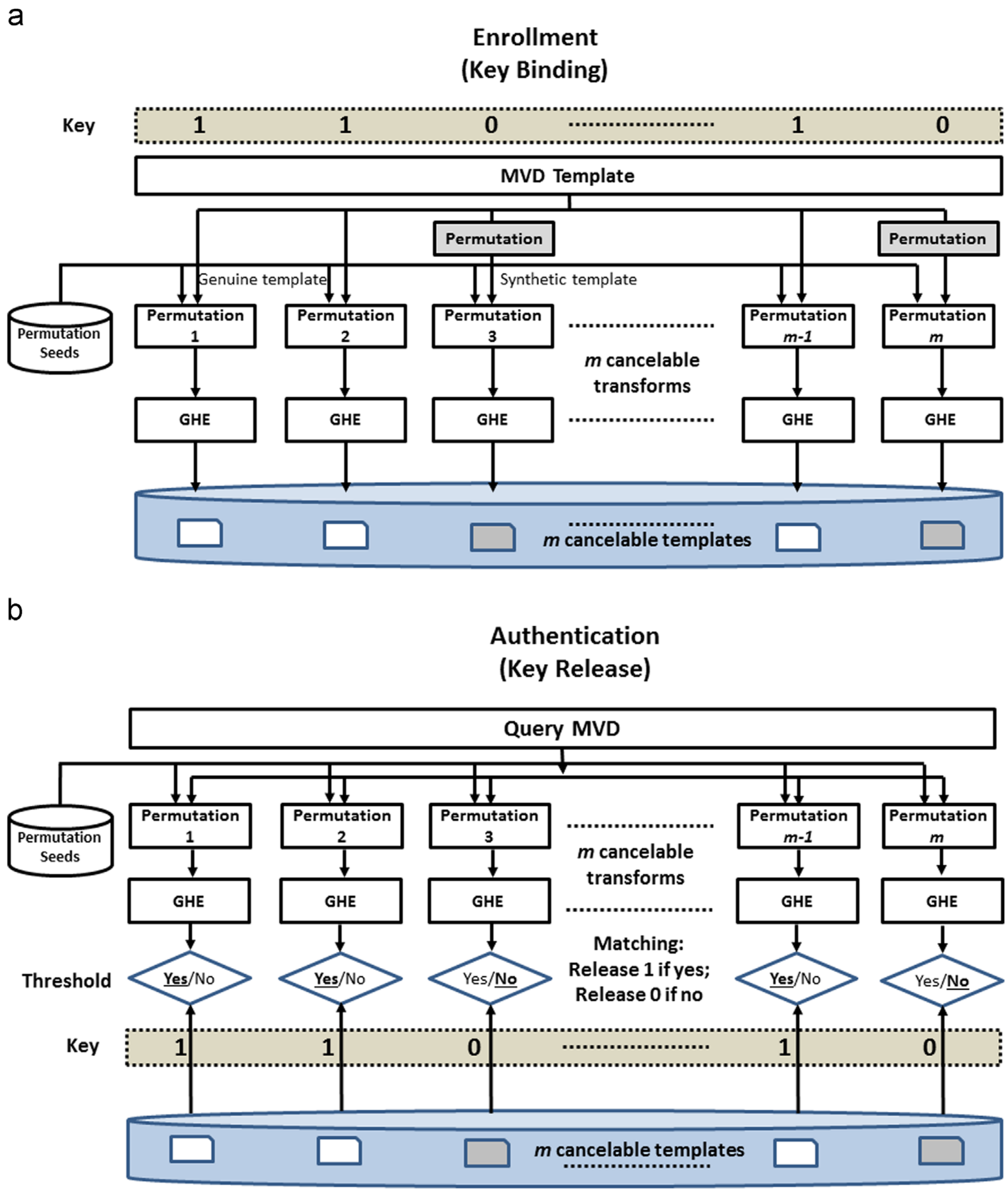


Fig. 3. Diagrams for the proposed key binding scheme: (a) demonstrates the key binding with biometrics data that comprises of true template and synthetic template; (b) depicts the key release by presenting a query biometric template. (a) Key Binding (b) Key Release.

template as described in Eq. (3).

$$\boldsymbol{\Omega}_{j,i} = \begin{cases} \text{Perm}\left(\boldsymbol{\Omega}_{\boldsymbol{i}}^{\boldsymbol{e}}\right) & \text{if} \quad k_j = 1 \\ \text{Perm}\left(\boldsymbol{\Omega}_{\boldsymbol{i}}^{\boldsymbol{s}}\right) & \text{if} \quad k_j = 0 \end{cases} (j = 1, \ldots, m), (i = 1, \ldots, N) \qquad (2)$$

$$\boldsymbol{\Omega}_{j,i} = \text{Perm}\left(\boldsymbol{\Omega}_{\boldsymbol{i}}^{\boldsymbol{q}}\right)(j = 1, \ldots, m), (i = 1, \ldots, N) \qquad (3)$$

where $\boldsymbol{\Omega}^s$ and $\boldsymbol{\Omega}^e$ represent the synthetic and true templates, respectively and Perm(.) denotes the random permutation function. $\boldsymbol{\Omega}_{j,i}$ refers to the i-th row of minutiae vicinity decomposition (MVD) for the j-th random permutations and N is the total number of vicinities extracted from minutia set. The permutation seeds applied on key binding are kept, which are used in key release stage in the identical order. Note that permutation in Eq. (2) and Eq. (3) is different from Eq. (1) as the latter is meant for generating synthetic template and the seed will be discarded right after used.

2) ***Non-invertible feature transform***. The non-invertible transform is to ensure: (1) the key is strictly concealed; (2) the restoration of minutiae is computationally hard. For (1), the recovery of transformed template $\boldsymbol{\Xi}$ should be difficult to avoid key leakage. If $\boldsymbol{\Xi}$ is inverted and parameters of permutation function are learned by the adversary, the original features $\boldsymbol{\Omega}$ can be restored thereafter. Once the entire set of $\boldsymbol{\Xi}$ is restored, the complexity of key retrieval reduces to 2^1 as only true and synthetic templates are used for key encoding. For (2), the fingerprint minutiae should not be recovered from $\boldsymbol{\Xi}$. For instance, fingerprint minutia should not be learned from a compromised $\boldsymbol{\Xi}$. This is consistent to the non-inveritiblity criterion for template

protection. Therefore, non-invertible transform is a critical construct for our key binding scheme.

3. Implementation

3.1. Revisit of MVD and RGHE

In our implementation, a modified randomized graph-based Hamming embedding transform (RGHE) is used to transform the fingerprint minutia into a non-invertible form. The original randomized graph-based Hamming embedding (RGHE) [36] generates a cancellable fingerprint template for protecting the geometric invariant features, namely minutiae vicinity decomposition (MVD) [35]. Prior to the details of the implementation, we briefly revisit the MVD and the RGHE.

3.1.1. Minutiae vicinity decomposition (MVD)

MVD [35] is a minutia descriptor constructed based on a set of minutia vicinity centered at the reference minutia. Given a set of fingerprint minutiae, $\{fm_i|i=1, \ldots,N\}$, a minutia vicinity V_i is defined as fm_i together with three nearest neighboring minutiae c_{i1}, c_{i2}, c_{i3} (measured with Euclidean distance), i.e. $V_i=\{fm_i, c_{i1}, c_{i2}, c_{i3}|i=1,\ldots,N\}$. Each minutia vicinity is then decomposed into four minutiae triplets $\{T_{ir}|i=1,\ldots,N, r=1, 2, 3, 4\}$. We select the length of three sides, the three internal angles and the relative orientation between two adjacent minutiae. Hence, a feature vector consists of nine features, which can be described as follows:

$$\boldsymbol{v_r} = (s_1, \alpha_1, \Delta o_1, s_2, \alpha_2, \Delta o_2, s_3, \alpha_3, \Delta o_3,) \tag{4}$$

where s_1, s_2, and s_3 denote the length of the three sides in pixel; α_1, α_2 and α_3 represent the internal angles measured in degree; $\Delta o_1=|o_1-o_2|$, $\Delta o_2=|o_2-o_3|$, and $\Delta o_3=|o_3-o_1|$ denote the relative orientation between two adjacent minutiae, where o_1, o_2, o_3 are the orientations for minutiae m_1, m_2, m_3, respectively.

Noted that the features extracted from a single minutiae triplet form a 9-dimensional vector $\boldsymbol{v_r}$ (refer Eq. (4)). By concatenating four 9-dimensional vectors from the four minutiae triples of a minutia vicinity together, we obtain a vector $\boldsymbol{v}=[\boldsymbol{v}_1\ \boldsymbol{v}_2\ \boldsymbol{v}_3\ \boldsymbol{v}_4]$ of 36 feature components for a minutia vicinity. The above process is repeated for the entire vicinity set (say N times) and consequently, the entire MVD features are stored in a matrix, $\boldsymbol{\Omega}$ of size $N \times 36$.

3.1.2. Graph-based hamming embedding transform (GHE) Revisit

GHE [36] is a transformation with distance preservation. GHE offers strong non-invertible property to protect minutiae-based representation such as MVD. Let $\boldsymbol{\Omega} \in \mathbb{R}^{N\times 36}$ represents MVD feature matrix and random projection [61] is further performed to obtain $\hat{\boldsymbol{\Omega}} \in \mathbb{R}^{N\times 36}$. Let $\mathrm{G}=\{\mathbf{U},\mathbf{W}\}$ be a weighted graph with vertex $\mathbf{U}$ for $|\mathbf{U}|=N$ and weight matrix $\mathbf{W} \in \mathbb{R}^{N\times N}$. Each element w_{ij} of $\mathbf{W}$ signifies the global similarity of vertex pairs $(\mathbf{u}_i, \mathbf{u}_j)$, which is measured by $w_{ij} = exp(-\|\mathbf{u}_i-\mathbf{u}_j\|^2/\sigma^2)$, where σ is the bandwidth of a heat kernel [37]. The objective of GHE is to search a binary mapping function $\varphi(\mathbf{u}) \in -1, 1^{\hat{m}}$ that minimizes the average Hamming distance between the resultant $\hat{m}$-bits binary codes with respect to the minutia vicinities in the Euclidean space. This problem can be formulated by solving the following optimization problem [38]:

$$\min_{\varphi} \int \mathbf{W}\|\varphi(\mathbf{u}_i)-\varphi(\mathbf{u}_j)\|^2 p(\mathbf{u}_i)p(\mathbf{u}_j)\,d\mathbf{u}_i d\mathbf{u}_j \tag{5}$$

subject to

$$\varphi(\mathbf{u}) \in -1, 1^{\hat{m}}$$

$$\int \varphi(\mathbf{u})p(\mathbf{u})d\mathbf{u} = 0$$

$$\int \varphi(\mathbf{u})\varphi(\mathbf{u})^T p(\mathbf{u})d\mathbf{u} = 1$$

where $p(\mathbf{u})$ is the probability distribution of $\mathbf{u}$

The second constraint $\int \varphi(\mathbf{u})p(\mathbf{u})d\mathbf{u} = 0$ requires the flipping probability of each individual bit of the resultant binary code to be 0.5 and the third constraint $\int \varphi(\mathbf{u})\varphi(\mathbf{u})^T p(\mathbf{u})d\mathbf{u} = 1$ requires the bits to be uncorrelated. Although the optimization problem in Eq. (5) with the first constraint $\varphi(\mathbf{u}) \in -1, 1^{\hat{m}}$ is NP hard, several analytical solutions are available via spectral relaxation, such as *eigenfunctions* of the weighted Laplace-Beltrami operators defined on the manifolds [37].

Specifically, let L_p be a weighted Laplacian operator that maps a function φ to $\psi = L_p\varphi$ by $\psi(\mathbf{u})/\varphi(\mathbf{u}) = D(\mathbf{u})\varphi(\mathbf{u})p(\mathbf{u}) - \int_{\mathbf{s}} W(\mathbf{s},\mathbf{u})\varphi(\mathbf{s}) p(\mathbf{s})d\mathbf{s}$ with $D(\mathbf{u}) = \int_{\mathbf{s}} \mathbf{W}(\mathbf{u},\mathbf{s})p(\mathbf{s})d\mathbf{s}$. The minimization problem can be simplified by solving $L_p\xi = \beta\xi$ for a real-valued β where ξ is an eigenfunction of L_p.

The above problems can be solved based on the two assumptions: 1) $p(\mathbf{u})$ is a separable distribution; 2) each input feature is drawn from a uniform distribution. It is noted if $p(\mathbf{u})$ is separable, and the similarity between data points is defined by $w_{ij} = exp(-\|\mathbf{u}_i-\mathbf{u}_j\|^2/\sigma^2)$, then the eigenfunctions ξ of L_p have an outer product form. The "outer-product" eigenfunctions are merely products of eigenfunctions along different dimensions and their eigenvalue is simply the product of the eigenvalues of these dimensions. Therefore, the first assumption implies that we may construct an eigenfunction $\xi(\mathbf{u})$ of L_p using a product of 36 single-dimensional eigenfunctions, $\xi(\mathbf{u}) = \prod_{i=1}^{36}\xi(u_i)$ corresponding to each feature. The second assumption allows us to select the following eigenfunctions as the single-dimensional eigenfunctions of the single dimensional Laplacian L_p in small ϵ, which is well studied in spectral theory [38]:

$$\xi_k(x) = \sin\left(\frac{\pi}{2}+\frac{k\pi}{b-a}x\right) \tag{6}$$

$$\beta_k = 1 - e^{-\frac{\epsilon^2}{2}\left|\frac{k\pi}{b-a}\right|^2} \tag{7}$$

where x is a single-dimensional arbitrary real feature uniformly distributed in the range of $[a, b]$; and β_k is the corresponding eigenvalue of $\xi_k(x)$, which serves as an indicator for eigenfunctions selection for GHE mapping.

From the above description, a three-step algorithm for GHE can be formed: 1) Principal Component Analysis (PCA) alignment, 2) Eigenfunctions selection and 3) Eigenfunctions coding. PCA alignment enables Gaussian distribution function be separable by simply aligning the data along the axes by rotation. The second step is to compute $\hat{m}$ eigenfunctions via $\xi_i(\mathbf{y}) = \prod_{j=1}^{36}\xi_i\left(y_j\right)$ for $i=1,\ldots, \hat{m}$ according to Eq. (6), where $\mathbf{y}$ is the 36-dimensional PCA-aligned vector. This can be done by evaluating the k eigenvalues for each of the 36 PCA directions with Eq. (7) and sort the resultant $36k$ eigenvalues in ascending order. After discarding eigenfunctions with zero eigenvalue, we select $\hat{m}$ eigenfunctions with the $\hat{m}$ smallest eigenvalues from the remaining eigenfunctions and encode the features of each minutia vicinity into a $\hat{m}$-bits binary string via zero thresholding. The same process repeats for entire MVD feature matrix. Finally, an $N \times \hat{m}$ binary code is obtained.

3.2. Modified RGHE

It is noted that the original Randomized GHE [36], which consists of a combination of random projection and GHE, is for cancellable biometric template construction with strong non-invertible property. Yet, it is not tailored for key binding that required addressing different set of design requirements. In this paper, we modify the Randomized GHE as shown in Fig. 4. The modifications are described as follows:

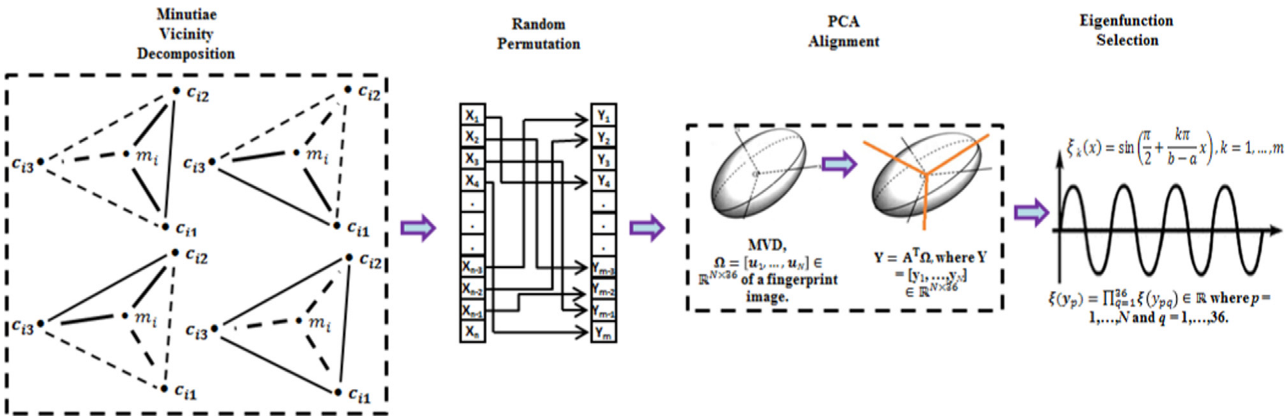

Minutiae Vicinity Decomposition
Random Permutation
PCA Alignment
Eigenfunction Selection
c_{i1}
c_{i2}
c_{i3}
m_i
X_1 X_2 X_3 X_4 X_{n-3} X_{n-2} X_{n-1} X_n
Y_1 Y_2 Y_3 Y_4 Y_{m-3} Y_{m-2} Y_{m-1} Y_m
MVD, $\Omega = [u_1, \ldots, u_N] \in \mathbb{R}^{N\times 36}$ of a fingerprint image.
$Y = A^T\Omega$, where $Y = [y_1, \ldots, y_N] \in \mathbb{R}^{N\times 36}$
$\xi_k(x) = \sin\left(\frac{\pi}{2} + \frac{k\pi}{b-a}x\right), k = 1, \ldots, m$
$\xi(y_p) = \prod_{q=1}^{36} \xi(y_{pq}) \in \mathbb{R}$ where $p = 1, \ldots, N$ and $q = 1, \ldots, 36$.

Fig. 4. Diagram of the modified randomized graph based hamming embedding (RGHE).

a. Instead of using random projection on MVD [35], we first random permute the minutia vicinity vectors within MVD matrix. The reason is that the range values of these vectors are nonhomogeneous since they are extracted from triangles (*length* of three sides, three internal *angles* and *orientation* difference). Therefore, random permutation is done by row-wise basis, $\hat{\boldsymbol{\Omega}}_{\boldsymbol{i}} = \text{Perm}(\boldsymbol{\Omega}_{\boldsymbol{i}}), i = 1, \ldots, N$, to preserve the characteristics of different features. $\boldsymbol{\Omega}_{\boldsymbol{i}}$ and $\hat{\boldsymbol{\Omega}}_{\boldsymbol{i}}$ represent the original and the permuted template respectively; N is the total number of vicinities extracted from minutia set.
b. Note the original GHE discussed in Section 3.1(B) applied a single-bit quantization scheme to convert the real-valued features to binary bits for speedy matching purpose [56]. However, the quantization does not preserve the Euclidean neighborhood structure effectively after mapping to Hamming space. In this paper, we omitted the quantization step and found that the accuracy can be gained, yet it would not compromise the non-invertible property significantly. The non-invertible property will be justified in Section 5.1. The details for the modified RGHE are given in Algorithm 3.

Algorithm 3. Modified randomize graph based Hamming Embedding.

```
Input Minutiae Vicinity Decomposition (MVD), $\boldsymbol{\Omega} \in \mathbb{R}^{N\times 36}$ and
  code length $\hat{m}$
Step 1: Random Permutation
1.1: $\hat{\boldsymbol{\Omega}} = \textbf{Perm}(\boldsymbol{\Omega}) \in \mathbb{R}^{N\times 36}$, Perm(.) denotes permutation
  function.
Step 2: PCA Alignment
2.1: Extracts eigenvectors $\boldsymbol{\Phi}$ from the covariance matrix,
  $\mathbf{C} = \hat{\boldsymbol{\Omega}}\hat{\boldsymbol{\Omega}}^{\mathbf{T}}$
2.2: Project $\hat{\boldsymbol{\Omega}}$ to eigenspace, i.e. $\mathbf{Y} = \boldsymbol{\Phi}^{\mathbf{T}}\hat{\boldsymbol{\Omega}}$, where $\mathbf{Y} = [\mathbf{y}_1, \ldots,$
  $\mathbf{y}_N] \in \mathbb{R}^{N\times 36}$
2.3: Calculate $a = \min(\mathbf{Y})$ and $b = \max(\mathbf{Y})$ for (6) and (7).
2.4: Calculate $36k$ eigenvalues from $\beta_k$ using (6) and sort them
  in ascending order.
Step 3: Eigenfunctions selection
3.1 Compute $\hat{m}$ eigenfunctions according to the $\hat{m}$ smallest
  eigenvalues from step 2.4, i.e.
  For $i = 1:\hat{m}$
    Compute $\xi_i(\mathbf{y}) = \prod_{r=1}^{36} \xi_i(y_r) \in \mathbb{R}$ as in (6).
  End for
3.2 Repeat Step 3.1 for all $N$ minutiae vicinities, hence
  $\boldsymbol{\xi}^{\boldsymbol{n}} = [\boldsymbol{\xi}_1, \ldots, \boldsymbol{\xi}_{\hat{m}}]$, where $n = 1, \ldots, N$.
Output Resulting template $\boldsymbol{\Xi} = [\boldsymbol{\xi}^{\boldsymbol{1}}, \ldots, \boldsymbol{\xi}^{\boldsymbol{N}}] \in \mathbb{R}^{N\times \hat{m}}$
```

3.3. Matching

After executed Algorithm 3, a template, $\boldsymbol{\Xi}$ with size $N \times \hat{m}$ can be formed, where N is the number of minutiae vicinity. The dissimilarity of enrolled and query templates, $\boldsymbol{\Xi}_e = [\boldsymbol{\xi}_{e1}, \ldots, \boldsymbol{\xi}_{eN_1}] \in \mathbb{R}^{N_1\times \hat{m}}$ and $\boldsymbol{\Xi}_q = [\boldsymbol{\xi}_{q1}, \ldots, \boldsymbol{\xi}_{qN_2}] \in \mathbb{R}^{N_2\times \hat{m}}$ can be computed by the smallest pairwise Euclidean distance between templates $\boldsymbol{\Xi}_e$ and $\boldsymbol{\Xi}_q$, where N_1 and N_2 are the number of vicinities extracted from an enrolled and a query fingerprint image. The score of a matched pair p_{ij} in the comparison of $\boldsymbol{\Xi}_e$ and $\boldsymbol{\Xi}_q$can be computed using Eq. (8). As such, a score matrix $\mathbf{P} = [p_{ij}]$ of size N_1 x N_2 can be obtained:

$$p_{ij} = \min\left(\left\|\boldsymbol{\Xi}_e, \boldsymbol{\Xi}_q\right\|\right) \tag{8}$$

where ||.|| denotes the Euclidean distance between $\boldsymbol{\Xi}_e$ and $\boldsymbol{\Xi}_q$.

Next, we store the *minimum value* for each row in $\mathbf{P}$, which is denoted as a_i:

$$a_i = \min_j\left(p_{ij}\right) \text{for } i = 1, \ldots, N_1 \text{ and } j = 1, \ldots, N_2 \tag{9}$$

The matching score can then be computed by counting the number of a_i that has a greater value than the pre-defined threshold t. To avoid large variation in the results caused by non-trivial difference in magnitude led by unstable number of minutiae in the query and enrolled images, the matching score can be normalized as follows:

$$s = \frac{\sum_{i=1}^{N1} (a_i < t)}{\sqrt{N_1 \times N_2}} \tag{10}$$

Hence, the score obtained is the real-valued score and the value '0' indicates a strong negative match and vice versa.

4. Experimental results

The experiments were conducted on five public fingerprint datasets, FVC2002 (DB1, DB2, DB3 and DB4) [39] and FVC2004 DB2. Each dataset consists of 100 users with 8 samples per user. In total, there are 800 (100 × 8) fingerprint images for each dataset. VeriFinger 7 SDK [40] was used for minutia extraction. The minutiae template is extracted according to ISO-complaint format for evaluation, i.e. (x, y, θ). The accuracy performance is evaluated using False Acceptance Rate (FAR), False Reject Rate (FRR), Genuine Acceptance Rate (GAR) as well as the receiver operating characteristic (ROC) curves.

In our experiment, we adopted two testing protocols: 1) *1vs1 protocol*: the first and second impressions of each subject are used

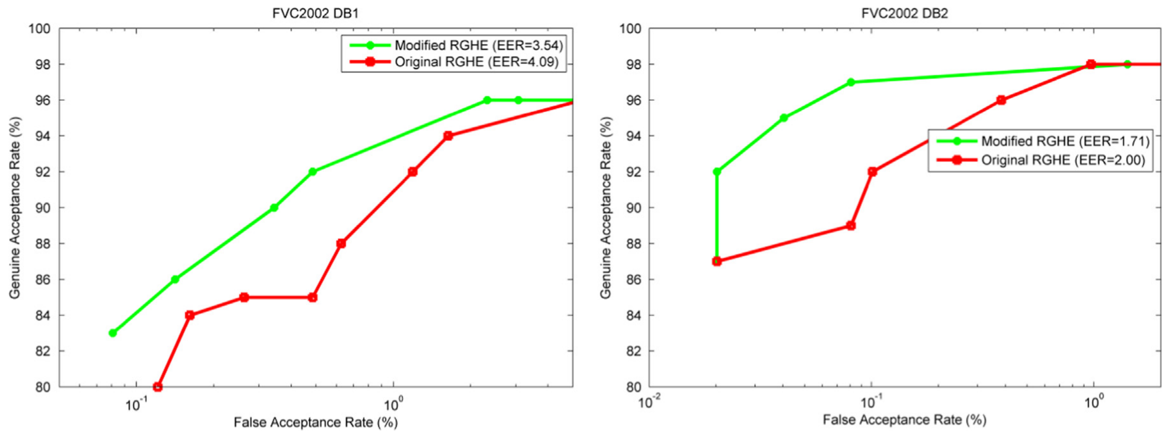


Fig. 5. ROC curves are served as comparison of the accuracy performance of the original RGHE and the modified RGHE for FVC2002 DB1 and DB2.

Table 1
Key release error rate for the proposed key binding scheme when the key length is increased.

Databases	Key-length (bits)	Random Permutation + GHE				Random Projection + GHE			
		1vs1 protocol (1st and 2nd images)		1-8 protocol (1st to 8th images)		1vs1 protocol (1st and 2nd images)		1-8 protocol (1st to 8th images)	
		FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)
FVC2002 DB1	1	0.16	11	0.12	26.57	0.18	11	0.26	23.71
	16	0.16	11	0.12	26.57	0.1	11	0.55	23.14
	32	0.16	11	0.12	26.57	0.1	11	0.30	25.14
	64	0.16	11	0.12	26.57	0.02	11	0.12	25.71
	128	0.16	11	0.12	26.57	0.02	12	0.10	27.86
FVC2002 DB2	1	0.061	3	0.12	13.14	0.16	2	0.34	13.29
	16	0.061	3	0.12	13.14	0.04	2	0.10	13.29
	32	0.061	3	0.12	13.14	0.02	3	0.20	13.14
	64	0.061	3	0.12	13.14	0.04	2	0.12	14.86
	128	0.061	3	0.12	13.14	0.02	2	0.10	15.29
FVC2002 DB3	1	1.25	25	3.45	27.14	0.71	33	0.99	41.43
	16	1.25	25	3.45	27.14	0.54	32	0.77	42.43
	32	1.25	25	3.45	27.14	0.48	33	0.79	41.71
	64	1.25	25	3.45	27.14	0.44	35	0.75	43.86
	128	1.25	25	3.45	27.14	0.40	35	0.77	44.71
FVC2002 DB4	1	1.49	21	3.47	21.86	0.57	38	0.97	33
	16	1.49	21	3.47	21.86	0.36	38	0.79	30.43
	32	1.49	21	3.47	21.86	0.26	38	0.79	29.14
	64	1.49	21	3.47	21.86	0.20	38	0.63	31.29
	128	1.49	21	3.47	21.86	0.14	38	0.55	32.43
FVC2004 DB2	1	1.89	45	3.07	45.86	1.73	45	1.27	50
	16	1.89	45	3.07	45.86	1.39	39	0.77	43.71
	32	1.89	45	3.07	45.86	0.93	39	0.77	44.29
	64	1.89	45	3.07	45.86	0.59	43	0.77	45.29
	128	1.89	45	3.07	45.86	0.42	45	0.69	51

as gallery and probe respectively. Due to the relatively good in image quality, this protocol is widely used for the experiments in biometric cryptosystems [27,41,50,51,59,60]. More precisely, such experimental setting can be justified that in biometric cryptosystems, the users are cooperative and willing to provide good quality biometric data to retrieve their cryptographic keys [18,26]. Hence, the matching yields 100 genuine scores and 4950 imposter scores; 2) *1-8 protocol*: the first impression of each subject is used as gallery and the rest of eight impressions of each subject are of probe. This protocol is to examine the robustness of the proposed method. Yet, we note that a poorer performance is anticipated with 1-8 protocol as the performance gap between the biometric cryptosystems and conventional biometric recognition systems has been acknowledged in Section 1.1. This protocol results 700 genuine scores and 4950 imposter scores.

4.1. Accuracy performance of the modified RGHE

We first investigate the accuracy performance of the original RGHE and the modified RGHE. Fig. 5 shows the receiver operating characteristic (ROC) curves of the original RGHE and the modified RGHE. It can be observed that the accuracy performance of the latter is improved over the former. This experiment confirms the justification given in Section 3.1, where the accuracy improvement is attributed by the removal of quantization in RGHE.

4.2. The key release error rate (KRER) of the proposed key binding scheme

As discussed in Section 1.1(*A*), one of the main limitations of existing key binding is the security-performance tradeoff. However, such a tradeoff is eliminated in the proposed scheme. In this paper, the performance of key release is evaluated by a metric, namely key release error rate (KRER) that comprises of two common indicators, false acceptance rate (FAR) and false rejection rate (FRR). From Table 1, it is interesting to note that the KRER remains the same for key size m from 1, 16, 32, 64 to 128 bits. This surprising fact is attributed to the RGHE mechanism and two-stage matcher. First, row-wise permutation of MVD vectors within the MVD, described in Eq. (2) and Eq. (3) is invariant with respect to the two-stage matcher (Section 3.3). Recall in two-stage matcher, the pairwise distances of row minutiae vicinity vectors are first exhaustively computed and the minimum value is taken for verification with respect to a chosen threshold value. Therefore, permutation would not alter the resulting KRER. This characteristic propagates to the stage of matching of two cancellable templates if the non-invertible transformation adopted in this scheme, i.e. modified RGHE, could preserve the pairwise relative distances of row minutia vicinity vector of a MVD after transformation. From the experiments results, we notice that this assumption is hold for RGHE (performance preservation before and after transformation [38]). Since all m distance scores are computed from the matching of m *permuted* cancellable templates and query input pair and all of them render *identical* distance scores, this implies that the KRER remains the same regardless m.

Table 2
Accuracy comparison between the proposed key binding scheme with the state-of-the-arts using 1 vs 1 protocol.

Methods	Accuracy for FVC2002-DB1 (%)	Accuracy for FVC2002-DB2 (%)
Proposed	**FRR = 11 (GAR = 89); FAR = 0.16**	**FRR = 3 (GAR = 97); FAR = 0.061**
	Security - identical to key length)	**(Security - identical to key length)**
Fuzzy Vault for fingerprint		
[18]	–	GAR = 91; FAR = 0.01; failure-to-capture rate (FTCR) = 2
[41]	–	GAR = 95; FAR = 0.01; failure-to-capture rate (FTCR) = 2
[50]	FRR = 19; FAR = 0.38 (14 bits security)	FRR = 17; FAR = 0.09 (25 bits security)
[51]	GAR = 85; FAR = 0.00 (29 bits security)	GAR = 93; FAR = 0.00 (32 bits security)
Fuzzy Commitment for fingerprint		
[42]	FNMR = 12.5; FMR = 0.1 (Approx. 43 bits security)	FNMR = 8.9; FMR = 0.1 (Approx. 43 bits security)
[27]	–	GAR = 85; FAR = 0.13 (Approx. 45 bits security)
[52]	FRR = 36.54; FAR = 0.29 (Approx. 143.2 bits security)	FRR = 26.48; FAR = 0.23 (Approx. 203.3 bits security)
[53]	FRR = 18.6; FAR = 0 (39 bits security)	FRR = 8.03; FAR = 0 (45 bits security)
Minutiae-based alignment-free bio-cryptosystems		
[59]	FRR = 8; FAR = 0.59 (Null)	FRR = 6; FAR = 0.02 (112 bits security)
[60]	FRR = 4; FAR = 0 (Approx. 33 bits security)	FRR = 2; FAR = 0 (Approx. 37 bits security)

To better illustrate this observation, let Ξ_1^e and Ξ_1^q be the 1st cancellable templates for enrolled and query pair and s_1 be the distance of Ξ_1^e and Ξ_1^q. Similarly, Ξ_2^e and Ξ_2^q be the 2nd permuted cancellable templates for enrolled and query pair and s_2 be the distance score of Ξ_2^e and Ξ_2^q. According to modified RGHE and two-stage matcher properties, it is known that Ξ_1^e and Ξ_2^e (also for Ξ_1^q and Ξ_2^q) are invariant with respect to the two-stage matcher, hence $s_1 = s_2$. By increasing the number of bits to m, the distance s_m of Ξ_m^e and Ξ_m^q is also identical to s_1 and s_2, i.e. $s_1 = s_2 = \dots s_m$. Since m distances among the cancellable templates $\Xi^e$and Ξ^q are identical, the key release operation resembles a single matching that repeated for m times. Thus, this explains why KRER remains unchanged with respect to m.

To further verify this observation, random projection [61] as a means of permutation function alternative, along with GHE is also examined and the KRERs are shown in Table 1. It can be observed that the KRERs for different m are no longer identical but slightly fluctuated. This is due to the row vectors in MVD after random projection is not exactly invariant to two-stage matcher despite the GHE still preserve the MVD structure.

Apart from the above, we have conducted an accuracy comparison experiment between the proposed scheme with state-of-the-arts [18,27,41,42,50,51,52,53,59,60] in fingerprint modality. Note that only FVC2002 DB1, DB2 and 1vs1 protocol are used for comparison as most of the literature [18,27,41,42,50,51,52,53,59,60] follows this protocol. We partitioned the state-of-the-arts of key binding schemes into three groups: i.e. fuzzy vault, fuzzy commitment and other alignment-free bio-cryptosystems. From the results shown in Table 2, our observations are summarized as follows:

1) For fuzzy vault, the accuracy of the proposed scheme is better than the works of [18,41,50,51]. Besides, there are two additional advantages provided by the proposed scheme: a) it is solely based on the minutiae information while the works [18] requires minutiae alignment based on the high curvature points and additional information such as ridge orientation, frequency required by [41]; b) a 2% of failure-to-capture rate (FTCR) in [18,41] is observed (e.g. failure for high curvature point extraction) while there is no failure-to-capture rate in our method since no additional information is utilized for performance improvement.
2) For fuzzy commitment, we observe that the KRER of the proposed scheme is comparable to the works [27,42,52,53]. Just to point out that for [27,42], additional information such as focal point of high curvature regions is mandatory for minutiae alignment.

Table 3
Key release error rate of the proposed key binding scheme by incorporating 2P-MCC using 1 vs 8 protocol.

Key-length (bits)	Key release error rate (FAR/FRR)(%)				
	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2004 DB1	FVC2004 DB2
1	0.06/3.29	0.06/2.57	0.83/16.71	0.99/17	0.73/16.43
16	0/2.29	0/1.57	0/10.57	0/15.71	0/16.29
32	0/2.43	0/1.57	0/11.71	0/16.14	0/14.42
64	0/2.43	0/1.71	0/12	0/16.86	0/15.14
128	0/2.43	0/1.86	0/13.29	0/17.29	0/16.86

3) For minutiae-based alignment-free bio-cryptosystems, our scheme outperforms [59] as observed in Table 2. Although a bio-cryptosystems recently reported by Yang et al. [60] shows an improvement both in security and accuracy performance. It is noticed that a helper data is exploited to reject the low quality

query sample for decoding. However, the failure-to-decode rate is not reported so that the comparison cannot be fairly justified without such information.

We further pointed out that the main objective of this paper is to demonstrate the feasibility of the proposed key binding scheme using cancellable transforms with comparable accuracy performance. Nevertheless, the performance could be enhanced with an effective minutia descriptor derived from sole minutiae set. As a proof-of-concept, 2P-MCC [43], a cancellable fingerprint template derived from the state-of-the-art minutia descriptor, MCC [32] is adopted in place of MVD. Table 3 demonstrates that the proposed key binding scheme outperforms all the existing key binding schemes with 2P-MCC.

4.3. Cancelability

Cancelability in this paper refers to two scenarios: 1) if the cryptographic key is compromised, a new key can be re-issued and the KRER should be preserved; 2) if the random permutation seeds for cancellable templates generation are compromised, a set of new seeds is issued to generate cancellable templates and the decoding accuracy should be preserved as well. Two experiments have been designed to evaluate the cancelability under these scenarios.

4.3.1. Cancelability in cryptographic key compromise scenario

We generated 100 sets of key randomly; each set consists of four keys with 16, 32, 64 and 128 bit-length respectively. We follow the same experimental protocol described in Section 4.2 to evaluate the KRER by changing the keys repeatedly. It is observed that the KRER is identical to what we have presented in Section 4.2. This is expected, in fact, whether a key can be released correctly is subjected to the matching result of two cancellable templates as shown in Fig. 3. Key changing would not affect the KRER as they are completely independent.

4.3.2. Cancelability in permutation seed compromise scenario

On the other hand, to assess the cancelability in permutation seed compromise scenario, we also randomly generated 100 sets of random permutation seeds and perform the experiment described in Section 4.2 by changing the permutation seeds. Note that 100 sets of random permutation seeds produce 100 sets of cancellable template to bind and release the cryptographic key. As expected, the KRER is identical to the accuracy presented in Section 4.2. The accuracy preservation is due to the modified RGHE mechanism and two-stage matcher as discussed before. Row-wise permutation in MVD by changing the seeds is invariant to the two-stage matcher and thus the distance between two MVD is identical. Further, it has been shown that the characteristics of GHE (i.e. structure preservation of MVD before and after transformation [38]) could preserve the relative distances propagated from MVD features. This is to prove the cancellable property in permutation seed compromise scenario is indeed achievable.

Table 4
Average time of encoding and decoding for the proposed key binding method in different bit-length.

Databases		Encoding (s)	Decoding (s)
FVC2002 DB1	16 bits	0.1183	0.1042
	32 bits	0.2509	0.2231
	64 bits	0.4932	0.4360
	128 bits	1.0013	0.8601
FVC2002 DB2	16 bits	0.1477	0.1385
	32 bits	0.2896	0.2672
	64 bits	0.5744	0.5417
	128 bits	1.1522	1.0757

4.4. Complexity analysis

We have also investigated the time complexity on encoding and decoding and the results are shown in Table 4. The average time is captured by the experimental machine with Intel i7 (3.4 GHz) CPU and 4 GB RAM. It can be observed from Table 4 that the average time of encoding and decoding is proportional to the bit-length of cryptographic key, which is straightforward due to the fact that more bits of the key requires more time for encoding or decoding. In general, the time efficiency for our key binding method is feasible for deployment.

5. Security and privacy analysis

In this section, we investigated the security and privacy of the implementation for the proposed key binding scheme. More precisely, the terms of privacy in this context refer to non-invertibility, non-linkability respectively while security refers the attacks for illegitimate access. As such, the analysis on the non-invertibility of the modified RGHE, Attacks via record multiplicity (ARM), Surreptitious Key-Inversion Attack (SKI) and statistical attack are given.

5.1. Non-invertibility of the modified RGHE

The non-invertibility in this context refers to the computational hardness of recovery of MVD features from the cancellable templates. This is to ensure that the original minutiae are securely protected (privacy preserving) and the spoofed impersonation derived from MVD is infeasible (security).

The non-invertibility of the modified RGHE is spurred by: 1) the sinus function $\xi_k(x) = \sin\left(\frac{\pi}{2} + \frac{k\pi}{b-a}x\right)$ in Eq. (6) offers many-to-one mapping capability and 2) the stacked product of 36 eigenfunctions i.e. $\xi(\mathbf{u}) = \prod_{i=1}^{36} \xi(u_i)$. We first investigated the many-to-one property of $\sin(\theta)$ where $\theta = \frac{\pi}{2} + \frac{k\pi}{b-a}x$ by conducting the following experiments: a) compute the mean and standard deviation of the angle θ from each MVD feature matrix; b) Since there are 800 MVD feature matrices derived from each dataset, we further compute the average mean and average standard deviation from the 800 MVD feature matrices. The results presented in Table 5 show that the angle (in rad) is invalid for the small angle approximation analysis [36] while the many-to-one property of RGHE is effective as the mean and the range of angle indicate that multiple solutions exist (i.e. θ exceeds 2π).

Secondly, to evaluate the invertibility of $\xi_i = \prod_{r=1}^{36} \sin\left(\frac{\pi}{2} + \frac{i\pi}{b-a}y_r\right)$, it is common to assume that ξ_i is known in the analysis (e.g., after database is compromised). The hardness of inverting ξ_i lies in the possible number of input θ of the sinus function. In Table 5, it is known that there are 8 and 10 possible inputs θ

Table 5
Mean and standard deviation for θ in Radian.

Measurements	**FVC2002 DB1**	**FVC2002DB2**
Average Mean of angle (rad)	11.6851	13.0572
Average S.T.D of angle (rad)	8.7962	10.6427
Range of angle (rad)	≈ 1.57 to 48.69	≈ 1.57 to 67.54
Maximum number of possible inputs corresponding to an output of a single-dimensional eigenfunction	8	10

associated with ξ_i for FVC2002 DB1 and DB2, respectively. Hence, for FVC2002 DB1 and DB2, the invertibility complexity for single minutia vector decomposition is upper bounded by $8^{36} \approx 2^{118}$ and $10^{36} \approx 2^{129}$, yielding 118 and 129 bits entropy, respectively. To invert N number of vicinities, the total invertibility complexity is therefore upper bounded by $8^{36}N \approx 2^{118}N$ and $10^{36}N \approx 2^{129}N$, yielding $118+\log_2(N)$ and $129+\log_2(N)$ bits entropy for FVC2002 DB1 and DB2, respectively.

Additionally, the user privacy in this context is highly concerned due to the fact that minutiae points can be used to reconstruct the fingerprint image easily [23]. To prevent the privacy leakage, the fingerprint minutiae points have to be protected securely. To do this, the MVD features reversal from the stored cancellable templates must be strictly prevented. This is equivalent to non-invertiblity problem of RGHE reasoned above. It has been demonstrated that such reversal is indeed infeasible due to computational hardness. Even in the event that MVD features are disclosed, converting the minutiae descriptor with invariant features into the absolute location and orientation of a minutia are rather challenging based on the existing techniques (e.g. Hill climbing). For example, a hill climbing approach may generate many spurious minutiae outside the region of interests (ROI) of the fingerprint image. Such reconstructed minutiae points may not lead to a high match score with another impression of the same finger [10].

5.2. Surreptitious Key-Inversion Attack (SKI)

As discussed in Section 2.3, the key can be retrieved only if the entire set of cancellable templates is successfully reversed to the true and synthetic templates. The effort to recover the MVD features from a single cancellable template requires 118 and 129 bits entropy respectively (see Section 5.1). Therefore, the full recovery for a single key with length m requires 118^m and 129^m ($m \geq 128$) trials respectively. Therefore, the SKI attack is computationally infeasible.

5.3. ECC-based attacks

5.3.1. Attacks via record multiplicity (ARM)

ARM in fuzzy commitment refers the decodability attack that we have discussed in Section 1.1 (A). In principle, ARM is feasible with high possibility due to the limitations of error correction codes employed. However, ARM is not possible in the proposed method as no ECC is employed.

We further point out that without the knowledge of key, the adversary is still difficult to distinguish the cancellable templates generated from true template or synthetic template. Thus, the correlation analysis among the cancellable templates generated from true templates cannot be performed. As such, it can be reasoned that ARM on the set of cancellable templates is indeed infeasible.

5.3.2. Statistical attack

Similarly, statistical attack discussed in Section 1.1 is also an ECC triggered attack. However, this attack is absent in the proposed key binding scheme due to the abandon of ECC. Further, statistical analysis on cancellable templates is hardly feasible due to 1) without cryptographic key, no clue of cancellable templates generated from true or synthetic template; 2) cancellable templates produced by RGHE are statistical indistinctive as discussed in Section 2.3.

6. Conclusion

In this paper, we proposed a ECC-free key binding scheme along with cancellable transforms for minutiae-based fingerprint biometrics in place of fuzzy commitments. The key binding process is accomplished by employing a series adoptive cancellable transforms and thresholding mechanism, which enjoys several merits. Firstly, the security-performance tradeoff that attributed by ECC is resolved in the proposed key binding scheme. This is confirmed by the extensive experiments where the accuracy performances remain stagnant regardless the increment of key size. Secondly, unlike fuzzy commitment, the scheme does not impose any restriction to the representation form of biometrics and hence matchers. A great flexibility of adopting effective feature extractors and robust matchers can be attained. Thirdly, the security and privacy of the proposed key binding construct that associated to non-invertibility and non-linkability criteria are justified. While ECC-free key binding scheme is still a new direction to study, we believe that the proposed scheme has wide room to improve in security, privacy and accuracy performance aspects in the future. We hope this work can provoke thoughts and discussions in this area.

Conflict of Interest Statement

None declared.

Acknowledgment

This research was partly supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and Future Planning (2013006574), Universiti Tunku Abdul Rahman Research Fund (IPSR/RMC/UTARRF/2013-C2/G04), eScience (01-02-11-SF0201), MOSTI, Malaysia and Anhui Provincial Project of Natural Science (KJ2014A095).

References

[1] C. Adams, S. Lloyd, Understanding the Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations, 1st ed., New Riders Publishing, Indianapolis, USA, 1999.

[2] A.K. Jain, 50 years of biometric research: the (almost) solved, the unsolved, and the unexplored, In: Proceedings of the 5th International Conference on Biometrics, keynotes, Madrid, Spain, June, 2013.

[3] A. Juels and M. Wattenberg, A fuzzy commitment scheme, In: Proceedings of the 6th ACM Conference on Computer and Communications Security, 1999, pp. 28–36.

[4] A. Juels and M. Sudan, A fuzzy vault scheme, In: Proceedings of IEEE International Symposium on Information Theory, Lausanne, Switzerland, 2002.

[5] A.K. Jain, K. Nandakumar, A. Biometric template security, EURASIP J. Adv. Signal Process. 2008 (2008).

[6] Y.J. Chang, W. Zhang, and T. Chen, Biometrics-based cryptographic key generation, In: Proceedings of IEEE International Conference on Multimedia and Expo (ICME 04), Taipei, Taiwan, vol. 3, 2004, pp. 2203–2206.

[7] C. Vielhauer, R. Steinmetz, and A. Mayerhofer, Biometric hash based on statistical features of online signatures, In: Proceedings of the International Conference on Pattern Recognition, Quebec, QC, Canada, vol. 1, 2002, pp. 123–126.

[8] Y. Dodis, L. Reyzin, and A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, In: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: advances in cryptology (EUROCRYPT 04), Lecture Notes in Computer Science, Interlaken, Switzerland, vol. 3027, 2004, pp. 523–540.

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

[10] A. Nagar, Biometric Template Security (Ph.D. dissertation), Dept. Comp. Sci. & Engn., Michigan State Univ, East Lansing, Michigan, USA, 2012.

[11] X. Zhou, A. Kuijper, R.N.J. Veldhuis, and C. Busch, Quantifying privacy and security of biometric fuzzy commitment, In: Proceedings of IEEE International Joint Conference on Biometrics, IJCB2011, 2011.

[13] W.J. Scheirer and T.E. Boult, Cracking fuzzy vaults and biometric encryption, In: Proceedings of the Biometrics Symposium, Baltimore, USA, 2007, pp. 1–6.

[14] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, G. Zemor, Theoretical and practical boundaries of binary secure sketches, IEEE Trans. Inf. Forensics Secur. 3 (2008) 673–683.

[18] K. Nandakumar, A.K. Jain, S. Pankanti, Fingerprint-based fuzzy vault: implementation and performance, IEEE Trans. Inf. Forensics Secur. 2 (4) (2007) 744–757.

[23] C. Hill, Risk of masquerade arising from the storage of biometrics (Masters thesis), Australian National University, Canberra, Australia, 2001.

[24] F. Farooq, R. Bolle, T. Jea, and N. Ratha, Anonymous and revocable fingerprint recognition, In: Proceedings of IEEE Computer Vision and Pattern Recognition, June 2007, pp. 1–7.

[25] Z. Jin, A. Teoh, T.S. Ong, C. Tee, A revocable fingerprint template for security and privacy preserving, KSII Trans. Internet Inf. Sys. 4 (6) (2010) 1327–1341.

[26] H. Xu, R. Veldhuis, A. Bazen, T. Kevenaar, A. Akkermans, Gokberk, Fingerprint verification using spectral minutiae representations, IEEE Trans. Inf. Forensics Secur. 4 (3) (2009) 397–409.

[27] A. Nagar, S. Rane, and A. Vetro, Privacy and security of features extracted from minutiae aggregates, In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Dallas, Texas, USA, March 2010, pp. 524–531.

[29] B. Yang, and C. Busch, Parameterized geometric alignment for minutiae-based fingerprint template protection, In: Proceedings of the IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems (BTAS 09), 340-345, 2009.

[30] K. Simoens, C. M. Chang, and B. Preneel, Reversing protected minutiae vicinities, In: Proceedings of the IEEE 4th International Conference on Biometrics: Theory, Applications and Systems (BTAS 10), 2010, pp. 1–8.

[31] M. Ferrara, D. Maltoni, R. Cappelli, Noninvertible minutia cylinder-code Representation, IEEE Trans. Inf. Forensics Secur. 7 (6) (2012) 1727–1737.

[32] R. Cappelli, M. Ferrara, D. Maltoni, Minutia cylinder-code: a new representation and matching technique for fingerprint recognition, IEEE Trans. Pattern Anal. Mach. Intell. 32 (12) (2010) 2128–2141.

[33] S. Wang, J. Hu, Alignment-free cancellable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach, Pattern Recognit. 45 (12) (2012) 4129–4137.

[34] R.L. Rivest, Chaffing and Winnowing: Confidentiality without Encryption, MIT Lab for Computer Science, Massachusetts, Cambridge, USA, 1998 ⟨http://people.csail.mit.edu/rivest/pubs/Riv98a.pdf⟩.

[35] Z. Jin and Andrew B. J. Teoh, Fingerprint template protection with minutia vicinity decomposition, In: Proceedings of the International Joined Conference on Biometrics (IJCB), 2011, pp. 1–7.

[36] Z. Jin, M.H. Lim, A.B.J. Teoh, B.K. Goi, A non-invertible randomized graph-based hamming embedding for generating cancellable fingerprint template, Pattern Recognit. Lett. 42 (2014) 137–147.

[37] M. Belkin, P. Niyogi, Laplacian eigenmaps for dimensionality reduction and data representation, Neural Comput. 15 (6) (2003) 1373–1396.

[38] Y. Weiss, A. Torralba, R. Fergus, Spectral hashing, In: Neural Information Processing Systems, 2008.

[39] Fingerprint Verification Competition (FVC2002) Database. ⟨http://bias.csr.unibo.it/fvc2002/databases.asp⟩, 2002.

[40] VeriFinger Software. ⟨http://www.neurotechnology.com⟩.

[41] A. Nagar, K. Nandakumar, and A. K. Jain, Securing fingerprint template: fuzzy vault with minutiae descriptors, In: Proceedings of the 19th International Confrence on Pattern Recognition ICPR, December, 2008.

[42] K. Nandakumar, A fingerprint cryptosystem based on minutiae phase spectrum, In: Proceedings of IEEE International Workshop on Information Forensics and Security, Seattle, USA, 2010.

[43] M. Ferrara, D. Maltoni, and R. Cappelli, A two-factor protection scheme for MCC fingerprint templates, In: Proceedings of the 2014 International Conference on Biometrics Special Interest Group (BIOSIG), pp. 1–8, 2014.

[44] T. Ignatenko, Secret-Key Rates and Privacy Leakage in Biometric Systems (Ph.D. thesis), Eindhoven University of Technology, Eindhoven, Netherlands, 2009.

[45] A.D. Smith, Maintaining Secrecy when Information Leakage is Unavoidable (Ph.D. thesis), Massachusetts Institute of Technology, Massachusetts, Cambridge, USA, 2004.

[46] K. Simoens, P. Tuyls, and B. Preneel, Privacy weaknesses in biometric sketches, In: Proceedings of IEEE Symposium on Security and Privacy, IEEE Computer Society, 2009.

[47] E.J. Kelkboom, J. Breebaart, T.A. Kevenaar, I. Buhan, R.N. Veldhuis, Preventing the decodability attack based cross-matching in a fuzzy commitment scheme, IEEE Trans. Inf. Forensics Secur. 6 (1) (2011) 107–121.

[48] C. Rathgeb and A. Uhl, Statistical attack against iris-biometric fuzzy commitment schemes, In: Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2011, pp.23 –30.

[50] W. Yang, J. Hu, and S. Wang, A Delaunay triangle group based fuzzy vault with cancellability, In: Proceedings of the 6th International Congress on Image and Signal Processing (CISP), 2013, vol. 03, pp. 1676–1681.

[51] P. Li, X. Yang, K. Cao, X. Tao, R. Wang, J. Tian, An alignment-free fingerprint cryptosystem based on fuzzy vault scheme, J. Netw. and Comput. Appl. 33 (3) (2010) 207–220.

[52] J. Hartloff, J. Dobler, S. Tulyakov, A. Rudra, and V. Govindaraju, Towards fingerprints as strings: Secure indexing for fingerprint matching, In: Proceedings of the International Conference on Biometrics (ICB), 2013, pp. 1–6.

[53] P. Li, X. Yang, H. Qiao, K. Cao, X. Tao, E. Liu, J. Tian, An effective biometric cryptosystem combining fingerprints with error correction codes, Expert Sys. Appl. 39 (7) (2012) 6562–6574.

[54] F. Carter and A. Stoianov, Implications of biometric encryption on wide spread use of biometrics, In: Proceedings of the EBF Biometric Encryption Seminar, Amsterdam, The Netherlands, June 2008.

[55] E.J.C. Kelkboom, J. Breebaart, I. Buhan, R.N.J. Veldhuis, Maximum key size and classification performance of fuzzy commitment for gaussian modeled biometric sources, IEEE Trans. Inf. Forensics Secur. 7 (4) (2012) 1225–1241.

[56] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of fingerprint recognition, 2nd ed., Springer-Verlag, 2009.

[57] Wikipedia, chaffing and winnowing, ⟨http://en.wikipedia.org/wiki/Chaffing_and_winnowing⟩.

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

[59] W. Yang, J. Hu, S. Wang, M. Stojmenovic, An alignment-free fingerprint biocryptosystem based on modified Voronoi neighbor structures, Pattern Recognit. 47 (3) (2013) 1309–1320.

[60] W. Yang, J. Hu, S. Wang, A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement, IEEE Trans. Inf. Forensics Secur. 9 (7) (2014) 1179–1192.

[61] W.B. Johnson, J. Lindenstrauss, Extensions of Lipschitz mappings into a Hilbert space, In: Proceedings of the Conference in Modern Analysis and Probability (New Haven, Conn., 1982), Contemporary Mathematics 26, Providence, RI: American Mathematical Society, pp. 189–206, 1984.

Jin Zhe obtained his BIT (Hons) majoring in software engineering and MSc (I.T.) from Multimedia University (MMU), Malaysia. Currently, He is pursuing a Ph.D. in the Faculty of Engineering and Science, Universiti Tunku Abdul Rahman (UTAR), Malaysia. His research interest is Biometrics Security, particularly in fingerprint template protection.

Andrew Beng Jin Teoh obtained his BEng (Electronic) in 1999 and Ph.D degree in 2003 from National University of Malaysia. He is currently an associate professor in Electrical and Electronic Department, College Engineering of Yonsei University, South Korea. His research, for which he has received funding, focuses Biometric Security and Machine Learning. His current research interests are face recognition and biometric template protection. He has published more than 220 international refereed journals, conference articles, several book chapters and edited book volume. He is also a regular speaker at conferences, academic institutions, and corporations. He has been a reviewer for more than 30 journals and conferences. He has served conference committees worldwide.

Bok-Min Goi received his BEng degree from University of Malaya (UM) in 1998, and the MEngSc and PhD degrees from Multimedia University (MMU), Malaysia in 2002 and 2006, respectively. He is now the Dean and a professor in the Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman (UTAR), Malaysia. Ir. Prof. Goi is the Chairperson for Centre for Healthcare Science & Technology, UTAR. He was also the General Chair for ProvSec 2010 and CANS 2010, Programme Chair for IEEE-STUDENT 2012 and Cryptology 2014, and the PC members for many crypto/security conferences. His research interests include cryptology, security protocols, information & biometrics security, digital watermarking, computer networking and embedded systems design. He is a senior member of the IEEE and corporate member of the IEM, Malaysia.

Yong-Haur Tay obtained his BCompSc and MEng (Elect) from Universiti Teknologi Malaysia, and PhD from École polytechnique de l'université de Nantes, France. He is presently an Associate Professor in the Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman (UTAR), Malaysia. He is also the Head of Programme for Master of Information Systems and the Chairperson for Centre for Computing and Intelligent Systems (CCIS), UTAR. Yong Haur has been actively involved in university-industry collaborations and consultancies that involve the application of machine learning, pattern recognition and computer vision techniques. He serves as a technical consultant to several international and local companies, in commercialization of those technologies.