Fingerprint Template Protection with Minutia Vicinity Decomposition

Jin Zhe¹  Andrew Teoh Beng Jin²

¹Faculty of Information Science & Technology, Multimedia University, Malaysia
jin.zhe@mmu.edu.my

²School of Electrical & Electronic Engineering, Yonsei University, South Korea
bjteoh@yonsei.ac.kr

Abstract

Minutia vicinity representation was recently proposed by Yang & Busch to generate a protected fingerprint template scheme [14], the resultant protected template enjoys good accuracy and free from alignment. However, Yang and Busche’s scheme is highly likely reversible [18]. This paper proposed a new minutiae representation technique known as Minutia Vicinity Decomposition (MVD) whereby each minutia vicinity is decomposed into four minutia triplets. A set of geometrical invariant features can be extracted from the minutia triplet to construct a fingerprint template. The invariant features with random offsets salting mechanism enhance the reversibility, revocability as well as performance accuracy of the resultant protected fingerprint template. Promising experimental results on FVC2002 DB2 justify the feasibility of our proposed technique.

1. Introduction

The security and privacy of the biometric template are gaining more attention in consequence of the emergent of numerous biometric applications. One of the major concerns in biometric template protection is the revelation of the user’s privacy due to the strong binding between biometric template and the user’s identity. For instance, personal particulars could be tracked through biometric templates from one application to another by cross-matching between biometric databases. This is further complicated by the fact that biometrics cannot be reproduced or replaced when compromised. Due to these concerns, a biometric system with protected template is required immediate attention. Ideally, template protection schemes must fulfill the following requirements [1, 2]:

(a) Diversity. A protected template must not allow cross matching across different applications, thereby ensuring user’s privacy.
(b) Revocability. A new template can be reissued once the old protected template is compromised.
(c) Non-invertibility. It must be impossible or computationally hard to obtain the original biometric template from the protected instance and helper data.
(d) Performance. Satisfactory protected system performance accuracy in terms of False Rejection Rate (FRR) or False Acceptance Rate (FAR).

Among various biometric template protection schemes, fingerprint minutiae protection is of great interest due to its wide acceptance and usage in commercial fingerprint recognition systems. In literature, many minutiae-based fingerprint template protection schemes have been proposed. The reported schemes can be broadly divided into two categories, namely alignment based or alignment-free based approach.

For the alignment-based approach, a registration point (core or delta) is required to align the fingerprint image before further processing. A well-known instance was reported by Ratha et al. [3] wherein the fingerprint minutiae data is transformed by a sequence of three non-invertible transforms functions: Cartesian, Polar and surface folding. Although the three transformation functions were claimed to be non-invertible due to the many-to-one mapping property, a scheme proposed by Feng et al. [4] reveals that Ratha’s surface folding transforms is possibly degenerated when the transformed template and parameters are known to the attacker. “Fuzzy vault”, another popular instance, was proposed by Juels and Sudan [5], wherein secret can be regenerated only if both enrolled and query minutia data are substantially overlapped. Many improved versions of fuzzy vault have been proposed, such as [6, 7, 8].

Ang et al. [9] proposed a key-dependent transformation method wherein a line through the core point is first specified and the minutiae above the line are reflected symmetrically below the line. Different template can be obtained by changing the line orientation. Nagar et al. [10] presented a richer set of fingerprint features which consist of minutiae features, ridge orientation features and ridge wavelength features. This feature set is finally binarized into bit-string to represent user template.

In contrast to the alignment approach, no registration point is needed in the alignment-free approach. For example, Farooq et al. [13] presented an instance of a binary fingerprint representation. Their idea is based on the fact that fingerprints can be represented by a set of triangles derived from sets of three minutiae. Seven invariant features, the length of three sides, the three angles between the sides and minutiae orientations and the height of the triangles are deliberately extracted and further quantized...
and hashed into a length of $2^{24}$ bits bit-string. However, this method required exhaustive calculation for all the possible triplet invariant features which results in high computation cost. Ahmad et al. [17] proposed a pair-polar coordinate based fingerprint template protection scheme which explores the relative relationship of minutiae in a rotation and shift-free pair polar framework. Non-invertibility is achieved based on the many-to-one mapping relation. A random translation parameter is introduced to further distort the minutia distribution. Other registration point free approach can be found in [11, 12, and 16].

Recently, Yang and Busch [14] proposed a fingerprint template protection method based on minutia vicinity. In their method, the given $N$ minutiae $\{m_i \mid i=1, 2, ..., N\}$ are used to form a set of minutia vicinity $V_i = \{m_i, c_{i1}, c_{i2}, c_{i3}\}$ by including 3 nearest neighboring minutiae, $c_{i1}, c_{i2}$ and $c_{i3}$. Each minutia vicinity comprises of 12 orientation vectors, i.e. $m_i \rightarrow c_{i1}$, $m_i \rightarrow c_{i2}$, $m_i \rightarrow c_{i3}$, $c_{i1} \rightarrow c_{i2}$, $c_{i2} \rightarrow c_{i1}$, $c_{i2} \rightarrow c_{i3}$, $c_{i3} \rightarrow m_i$, $c_{i3} \rightarrow c_{i1}$, $c_{i3} \rightarrow c_{i2}$, $c_{i1} \rightarrow c_{i3}$, $c_{i1} \rightarrow c_{i2}$, $c_{i1} \rightarrow c_{i3}$. The 4 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 protected minutia vicinity with stored random offsets.

Despite of minutia vicinity representation and random offsets addition used in [14] enjoys several merits such as simplicity, good accuracy and alignment-free, Simoens et al. [16] pointed out that coordinates and orientations of minutia in Yang and Busch’s template are likely to be revealed if both random offsets and orientation vectors are available to the adversary. [16] also showed that the attack complexity is considerable low i.e. $2^{17}$ attempts are required when the adversary knows the random offsets table. Although Yang et al. used dynamic random projection which was originally outlined in [2] to alleviate this problem, dynamic random projection incurs substantially increased computation cost than that of random offsets addition in [14].

In this paper, we propose a minutia template protection scheme based on Minutia Vicinity Decomposition (MVD). Our proposal is to decompose each minutia vicinity into four minutia triplets, and a set of geometrical invariant features are extracted from each minutia triplet. The advantage of using the derived invariant features is of two-fold: (i) they are more discriminative and error tolerance, than that of mere vicinity structure used in [14], (ii) the invariant features are not reversible due to their weak relation to the coordinates and the orientations of the minutiae.

The rest of the paper is structured as follow: Section 2 presents the proposed method; Experimental result is presented and discussed in Section 3; Security analysis and conclusion are presented in Section 4 and 5.

2. Proposed Fingerprint Template with Minutia Vicinity Decomposition

In our scheme, minutia vicinity set is first constructed and each of the minutiae vicinity is then decomposed into four minutia triplets. Then, a set of randomized geometric invariant features are derived from the minutia triplets and stored as a template. Figure 1 shows the block diagram of our proposed scheme. Generally, our proposed fingerprint template protection scheme consists of five stages as follows:

(a) Minutia Vicinity Formulation
(b) Minutia Vicinity Decomposition
(c) Invariant Features Extraction
(d) Protected Template Formulation
(e) Template Matching

The detail of each stage will be presented in the following subsections.

2.1. Minutia Vicinity Formulation

The scheme exploited minutia vicinity which was presented in [14]. In particular, for a set of $N$ fingerprint minutia, $\{m_i \mid i=1, ..., N\}$, a minutia vicinity $V_i$ is defined as $m_i$ together with 3 nearest (measured in terms of Euclidean distance) neighboring minutiae $c_{i1}$, $c_{i2}$, $c_{i3}$, i.e. $V_i = \{m_i, c_{i1}, c_{i2}, c_{i3}\}$.

There are two advantages of using minutia vicinity: (i) alignment-free; minutiae vicinity characterizes a particular local area of fingerprint and it is invariant to the translation, rotation and scaling, thus does not require registration points which are difficult to detect accurately [3]; (ii) minutia vicinity is a subclass of the nearest neighbor-based structure which can lead to, fixed-length descriptors [1]. The variant instances of nearest neighbor-based structure can be found in [19, 20, 21, 22].

2.2. Minutia Vicinity Decomposition

However, the minutia vicinity is a weak representation when a genuine minutia is missing or a spurious minutia is allocated. For example, in Fig 1 (b), if the genuine minutia $c_{i1}$ (one of the nearest neighbor minutia) is missing, then the next nearest minutia is included in the minutiae vicinity, thus the structure of minutia vicinity is distorted. Similarly, a spurious minutia also can deform the structure for minutia vicinity. It should be noted that missing genuine minutia or present of spurious minutia are commonly occurred during the fingerprint image acquisition. To rectify this problem, each of the minutia vicinity is decomposed into four minutia triplets $\{T_{ir} \mid i=1, ..., N, r=1, 2, 3, 4\}$, as showed in Figure 1(c). Therefore, in the event of a genuine minutiae is missing or a spurious minutiae is allocated, the other three
genuine minutiae still retain as a genuine minutia triplet. Besides, compare with other polygons, triplet is a more stable and reliable structure of representation.

2.3. Invariant Features extraction

The stability of the triangles has been validated under rigid transformation [23, 24, 25]. Hence, the elastic deformation of fingerprint during image acquisition should not affect the triplet significantly [13]. Based on this fact, multiple robust invariant features associated with the minutia triplet can be derived. The possible list of invariant features can be the length of the sides, the internal angles, the angles between the sides and minutia orientation, triangle handedness, triangle height etc. In this paper, we select the length of three sides, the three internal angles and the relative orientation between two adjacent minutiae as shown in Figure 2 as the invariant features. Hence, a feature vector, \( \mathbf{u} \), which consists of nine features can be formed as follows:

\[
\mathbf{u}_r = (s_1, \alpha_1, \Delta \alpha_1, s_2, \alpha_2, \Delta \alpha_2, s_3, \alpha_3, \Delta \alpha_3) \quad \text{where} \quad r=1, \ldots, 4
\]

where \( \Delta \alpha_1 = |\alpha_1 - \alpha_2| \)

\( \Delta \alpha_2 = |\alpha_2 - \alpha_3| \)

\( \Delta \alpha_3 = |\alpha_3 - \alpha_1| \)

where \( s_1, s_2 \) and \( s_3 \) denote the length of the three sides in pixel; \( \alpha_1, \alpha_2 \) and \( \alpha_3 \) represent the internal angles measured in degree; \( \Delta \alpha \) denotes the relative orientation between two adjacent minutiae and \( \alpha_1, \alpha_2, \alpha_3 \) are the orientation for minutiae \( m_1, m_2, m_3 \) respectively. Fig 2 illustrates the invariant features extracted from minutia triplet.

2.4. Protected Template Formulation

The features extracted from a single minutia triplet result a 9-dimensional vector, \( \mathbf{u}_r \) as shown in (2). A matrix with size 9×4, \( \mathbf{U} = [\mathbf{u}_1 \ \mathbf{u}_2 \ \mathbf{u}_3 \ \mathbf{u}_4] \) can be formed from 4 minutia triplets. On the other hand, in order to achieve revocability, we adopt biometric salting [26] technique by adding a user-specific random matrix, \( \mathbf{R} \) which is stored in the token. In the event of a template is lost or compromised, the new one can be re-issued by using different random matrix. Mathematically, the feature vector after random offsetting can be defined as:

\[
\mathbf{W}_i = \mathbf{U}_i + \mathbf{R} \quad i=1, \ldots, N
\]

where \( \mathbf{R} \) denotes the random matrix and \( \mathbf{W}_i \) is the transformed feature matrix.

It should be noted that the feature matrix generated thus far is based on single minutia vicinity. The processes described from Section 2.1 to 2.4 are repeated for \( N \) times until the entire vicinity set was traversed. Consequently, the size of the resultant matrix is of \( N \times 4 \times 9 \).

2.5. Template Matching

The matching of two templates with different sizes, \( \mathbf{W}_i \) and \( \mathbf{W}_j \) where \( i \neq j \) is by seeking the two most similar randomised minutia triplets, ie. column vector \( \mathbf{w}_r \) of \( \mathbf{W}_i \) in (2), which can be quantified by the minimum Euclidean distance among a set of \( \mathbf{w}_r \). Hence, we devise an exhaustive searching strategy as follows. Let

![Figure 1: Block diagram for the proposed fingerprint template generated from the minutia vicinity decomposition.](image)

![Figure 2: Invariant features extraction from minutia triplet.](image)
be the feature matrices which are generated from \( n \)-th and \( m \)-th vicinity and there are \( N \) and \( M \) vicinities (minutia) in each enrolled and query fingerprint image, respectively.

The matched pair scores, \( p_{nm} \) of \( W^n \) and \( W^m \) can be determined using (3) and a matrix \( P = [p_{nm}] \) with size \( N \times M \) can be formed thereafter.

\[
p_{nm} = \min_{i,j=1,\ldots,N} (||w^n_{qi} - w^m_{qi}||) \quad n = 1,\ldots,N \text{ and } m = 1,\ldots,M \tag{3}
\]

where \( ||.|| \) denotes the Euclidean distance between \( w^n_{qi} \) and \( w^m_{qi} \). The matching process of (3) is illustrated in Fig. 3.

Next, we store the minimum value for each row in \( P \), denoted as \( a_n \),

\[
a_n = \min_m (p_{nm}) \quad n = 1,\ldots,N \text{ and } m = 1,\ldots,M \tag{4}
\]

The matching score is merely counting the number of \( a_n \) that is greater than a pre-defined threshold, \( t \). However, the enormous difference of magnitude defined by the total number of minutiae in query image and enrolled image is problematic. Hence, the matching score can be normalized as follows:

\[
s = \frac{\sum_{n=1}^{N} (a_n < t)}{\sqrt{N \times M}} \tag{5}
\]

Hence, the score ranges from 0 to 1 where a score is toward ‘1’ indicates a perfect match and otherwise.

3. Experimental Results

The experiments of the proposed scheme are conducted with a public fingerprint database FVC2002_DB2 [27] which consists of two subsets, Set A and Set B; Set A comprises 100 users and each user has 8 samples, hence there are 800 (100×8) fingerprint images in total; on the other hand, Set B comprises 10 users and 8 samples for each user, 80 fingerprint images in total. Set B is normally used for parameter tuning and validation purpose. VeriFinger 6.0 SDK [28] is used to extract minutiae from every fingerprint images. The performance of the proposed method is evaluated by employing Equal Error Rate (EER), genuine-imposter distribution and receiver operating characteristic (ROC).

3.1. Performances

The performances in two scenarios namely different-token and stolen-token scenario are evaluated. For different-token, each individual is assigned a random matrix, which is used to mix with feature matrix as shown in (2) and this random matrix is user specific. On the other hand, verification in the stolen-token scenario is a situation where a genuine user lost his/her random matrix stored in the token and an impostor has gained this information to perform verification. This is also known as Lost Token Attack.

Firstly, the optimal value of threshold \( t \) in (5) is sought. Figure 4 shows the receiver operating characteristics (ROC) curves with \( t = 0.5 \), \( t = 1 \) and \( t = 1.5 \). It can be observed \( t = 1 \) yields the best performance, thus it is used for the subsequent experiments. We noted that this experiment is conducted under stolen-token scenario with FVC2002_DB2 set B.

![Figure 4: ROCs serves a comparison among the performance of the different value of threshold \( t \)](image)

For the experiments in sequel, two protocols are designed:

(a) The first 100 samples in FVC2002_DB2_A were used as gallery and the 100 second samples are probes. Hence, the matching yields 100 genuine scores and 9900 imposter scores. This strategy is used to compare with other methods in literature which adopted the same strategy.

(b) We selected samples 1 as gallery and samples 2, 3, 6, 7 and 8 as probes for this experiment. We
removed samples 4 and 5 as they are exaggeratedly rotated, displaced and incomplete; and such images are unlikely present in practice as users should be aware of cooperation.

For protocol (a), Table 1 shows the performance result in terms of EER for the proposed method as well as other methods which adopted the same protocol and software (VeriFinger) for fingerprint minutia extraction. It can be observed that the proposed method offers better performance compared to Yang & Busch’s [14] and Ahmad et al.’s [17]. It is easily asserted that the performance of [14] suffers from spurious minutiae, i.e. the selected orientation vector is likely based on a spurious minutia then the shifting of the rest of genuine minutiae is severely distorted. The resultant feature vector is less discriminative and deteriorates the performance. On the other hand, the proposed method resists to spurious minutia and missing genuine minutia since the other three genuine minutiae are still retain as a genuine minutia triplet. Therefore, we reveal that besides radius-based structure [1], minutia vicinity approach (a subclass of nearest neighboring based structure) does tolerate spurious minutiae or missing genuine minutia by MVD. For Ahmad’s method [17], a pre-selected distance is used as threshold to select the minutiae points. However, this technique does not help on selecting the genuine minutia and excluding the spurious minutiae.

Table 1: Performance accuracy on FVC2002_DB2_A for protocol (a)

<table>
<thead>
<tr>
<th>Methods to be compared</th>
<th>EER % (Different-token)</th>
<th>EER % (Stolen-token)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our method</td>
<td>0.00</td>
<td>0.21</td>
</tr>
<tr>
<td>Yang and Busch [14]</td>
<td>4.04</td>
<td>-</td>
</tr>
<tr>
<td>Ahmad et al. [17]</td>
<td>-</td>
<td>5.00</td>
</tr>
</tbody>
</table>

Table 2: Performance accuracy on FVC2002_DB2_A for protocol (b) under stolen-token scenario

<table>
<thead>
<tr>
<th>Proposed Scheme</th>
<th>Test Set 1-2</th>
<th>1-3</th>
<th>1-6</th>
<th>1-7</th>
<th>1-8</th>
</tr>
</thead>
<tbody>
<tr>
<td>EER (%)</td>
<td>0.21</td>
<td>1.34</td>
<td>6.05</td>
<td>5.34</td>
<td>6.58</td>
</tr>
<tr>
<td>Average EER (%)</td>
<td>3.90</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average EER (%) of [29]</td>
<td>7.38</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Apart from accuracy, the computation time of the proposed scheme is also considerably low compared to [13]. Let \( N \) be the number of minutiae in a fingerprint image which results \( N \) minutia vicinity. After vicinity decomposition, there are 4N minutia triplets need to be processed. Assume that the 1 unit time is used to process 1 minutia triplet, the total computational time is of 4N. Compare to a well-known instance of sole minutia triplet scheme as in [13], it processes \( \frac{N^1}{(N-3)\times 2!} \) minutia triplets in total which is much higher than the proposed scheme. It is distinguishable between the proposed method with [13] in terms of final representation and matching technique. [13] converts the minutia set into bit string and thus hamming distance is used for matching. Our technique leverages geometrical invariant features and a specific metric was devised for matching. Therefore, our method does not need to apply quantization.

3.2. Revocability

To evaluate this criterion, 100 sets of random numbers are first generated. Subsequently, 100 different templates are generated from a single fingerprint image by replacing 100 sets of different random numbers. The 100 different templates are further compared with the genuine templates which reduces FRR; c) invariant features extracted from minutiae triplets are well adopted to the fingerprint elastic deformation [13, 23, 24, 25] from genuine users and sensitive to the imposter, thus FAR can be reduced.

Figure 5: ROCs for genuine vs. imposter and genuine vs. pseudo-imposter for FVC2002_DB2_A.
and the comparisons generate a distribution namely \textit{pseudo-impostor distribution}. To avoid statistical biasness, each fingerprint image in the dataset takes turns to be the source in generating the revocable template and the average EER is recorded. Specifically, 100 pseudo-impostor scores are generated for one template. Hence, 800 templates result in 80,000 (800×100) scores. As expected, we obtained a 0.396\% of average EER. The ROCs for the revocability experiments are shown in Figure 5.

![Figure 5: Genuine-impostor Distributions and Pseudo-impostor Distribution for FVC2002_DB2_A.](image)

Figure 6 depicts the three distributions, i.e. genuine, imposter and pseudo-impostor distributions of revocability experiment. It can be observed that there is a strong overlap between the impostor distribution and pseudo-impostor distribution. This implies that the templates generated with different tokens resemble the fresh new templates, even though they are originated from the same image source and the performance in terms of EER does not degraded. Therefore, the claim of revocability is vindicated.

### 3.3. Diversity

The experiment conducted in Section 3.2 shows that even though the 100 different templates are generated from a single fingerprint image, they can still significantly be distinguished from the original template. That means individual can enroll different templates using the same finger at different physical applications without cross-matching. Therefore, the experiments conducted in Section 4.1 do not only vindicate the claim of revocability but also to validate the property of diversity.

### 4. Security Analysis

Non-invertibility in our context refers to the computational hardness in recovering the fingerprint minutia from the protected template and/or random matrix. As such, two criteria, namely \textit{weak privacy} and \textit{strong privacy} are discussed. Weak privacy refers to the computational hardness in reconstructing the fingerprint minutiae if the token is known. On the other hand, strong privacy refers to the difficulty in reconstructing the fingerprint minutiae when both token and protected templates are revealed to the adversary.

In the weak privacy criterion, the random matrix, \( R \) is gained by an adversary. Since \( R \) by no means associate with the feature matrix, \( U \) according to (2), the adversary is clueless to learn anything about \( U \) with \( R \) alone.

For strong privacy concern, it is assumed that potential adversaries are in knowledge of parameter and algorithm as well as gains both protected template, \( W \) and random matrix, \( R \). Feature matrix, \( U = (W - R) \) which consists of a set of geometrically invariant features, \( U = [u_1, u_2, u_3, u_4] \) would be revealed easily. Since each \( U \) contains 4 minutia triplets geometrical information which were derived from a minutia vicinity, \( V_i \), the minutiae recovering and estimation are now boiled down to a combinatorial attempt of minutia vicinity construction due to the weak relation of minutia vicinity - a spatial topological structure and individual minutiae location and orientation.

If we assume that the average size of \( V_i \) is approximately 50×50 pixels while the size of original images used in this experiment is 296×560 pixels. The effort of guessing the correct local area of \( V_i \) within the original image requires around \((296-50) \times (560-50) = 246 \times 510 = 125460\) attempts. Furthermore, \( V_i \) has possible 360 rotation degrees, thus the number of attempts increase to 45165600. Moreover, this estimation is limited to spatial location (i.e., \( x \) and \( y \)) while the minutia orientation should also be considered. Since \( U \) contains 6 orientation differences, \( \pm \Delta o_1, \pm \Delta o_2 \) and \( \pm \Delta o_3 \), the total attack complexity for \( V_i \) is approximately \( 45165600 \times 6 = 270993600 \approx 2^{27} \) attempts. Therefore, the attack complexity of the proposed scheme is significantly higher than that of \( 2^{17} \) attempts in [14] when both token and protected templates are available to the adversary.

### 5. Conclusion

In this paper, we proposed a fingerprint template protection scheme using minutia vicinity decomposition technique. The experimental results suggest that the proposed scheme provides the satisfactory performance accuracy and revocability in FVC2002_DB2_A. We also discussed the security concerns for the proposed scheme, particularly in template irreversibility. The analysis showed that it is computationally hard to retrieve minutia information even when both protected template and random matrix are known. Besides that, the scheme is free from alignment and light in complexity. Analysis on the geometric decomposition technique in the nearest neighbor-based structure would be our future research direction.
Acknowledgements

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST) (No. 2011-8-1095).

References