A Novel Fingerprint Template Protection Scheme Based on Distance Projection Coding

Ruifang Wang1,2, Xin Yang2, Xia Liu1
School of Automation
1Harbin University of Science and Technology
Beijing, P.R. China
wangruifang@fingerpass.net.cn

Sujing Zhou2, Peng Li2, Kai Cao2, and Jie Tian1
Center for Biometrics and Security Research
2Institute of Automation, Chinese Academy of Sciences
Beijing, P.R. China
tian@fingerpass.net.cn

Abstract—The biometric template, which is stored in the form of raw data, has become the greatest potential threat to the security of biometric authentication system. As the compromise of the biometric data is permanent, the protection of biometric data is particularly important. Consequently, biometric template protection technologies have aroused research highlights recently. One of the most popular template protection methods is biometric cryptosystem method. In this paper, we design a codebook named distance projection for biometric coding to generate secured biometric template, and propose a novel fingerprint biometric cryptosystem scheme based on the codebook. Experimental results on FVC2002 DB2 show that the proposed scheme can obtain positive results on both security and authentication accuracy.

Keywords—biometrics; template protection; codebook

I. INTRODUCTION

Recently, biometric template protection technologies have aroused research highlights. The main difficulty of biometric template protection lies on the fuzziness of biometrics. Unlike familiar cryptographic techniques, biometric data is inexact and can only be approximately matched, and therefore cannot be protected by direct cryptographic operations. Particularly, for minutia feature of fingerprints, the fuzziness is more complicated because the distance of two feature vector cannot be represented by single Euclidean metric or set difference metric, but combining of the two kinds of metrics. Therefore, existing algorithms dealing with the fingerprint fuzziness mainly focus on removing Gaussian errors generated by Euclidean distance for the first step and burst errors generated by set difference distance for the second step [9][10].

There are some state-of-art algorithms adopted for removing burst errors [1][2]. However, algorithms to remove Gaussian errors are mainly based on fuzzy vault method [3][6], which mixed minutiae and randomly selected chaff points to generate secured fingerprint template. While the fuzzy vault-based template suffers biometric information leakage and cannot provide adequate security, Scheirer et al. [4] introduced three classes of attacks against biometric fuzzy vaults: attack via record multiplicity (ARM), surreptitious key-inversion (SKI) attack, and blended substitution attacks. Then Kholmatov et al. [5] made the realization of correlation attack against the fuzzy vault scheme successfully.

In this paper, we design a codebook named distance projection for biometric coding to generate secured biometric template and propose a novel fingerprint template protection scheme. The proposed scheme based on our coding method can remove Gaussian errors effectively and obtain promising authentication performance with a certain degree of security. Experimental results illustrate that the proposed fingerprint template protection scheme possesses practical value and also can be combined with methods for removing burst errors to construct a minutia-based key binding system.

The rest of the paper is organized as follows. In Section 2, we propose the construction details of our codebook for biometric coding. The fingerprint template protection scheme based on our coding method is given in Section 3. In Section 4, experimental results are presented. We do security analysis of the proposed scheme in Section 5. Finally, we finish with conclusion in Section 6.

II. CODEBOOK DESIGN FOR BIOMETRIC CODING

We design a codebook named distance projection for biometric encoding and decoding for Euclidean metric space. Given a real valued biometric feature vector $x=(x_1,x_2,...,x_l)$, where $l$ is the biometric feature length. Choose two vectors $K=(K_1,K_2,...,K_l)$ and $\lambda=(\lambda_1,\lambda_2,...,\lambda_l)$, we can obtain the following codeword space

$$C=\{k_1\lambda_1k_2\lambda_2...,k_l\lambda_l\} | k_i \in Z, 0 \leq k_i \leq K_i - 1, 1 \leq i \leq l \}$$

(1)

The vector $K$ is an integer vector to decide the size of codeword space, and its elements are decided by

$$K_i=\left[\frac{(x_{max}^i-x_{min}^i)}{\lambda_i}\right], 1 \leq i \leq l.$$  

(2)

where $\lambda_i$ is the quantization step.

The distance projection encoding procedure projects each element of the biometric feature vector onto the nearest codeword $z_i \in C_j$, which is decided by

$$z_i=\arg\min_{c_i \in C_j} |x_i-c_i|, 1 \leq i \leq l.$$  

(3)

Then we compute the difference between the element value and its corresponding codeword, i.e., $d_j=x_j-z_j$. And the codeword vector $z=(z_1,z_2,...,z_l)$ is used as a secret, while the difference vector $d=(d_1,d_2,...,d_l)$ is stored in the secured biometric template.

In the decoding procedure, given a query feature vector $x^\prime=(x_1^\prime,x_2^\prime,...,x_l^\prime)$ and the difference vector $d$, we first project each element of the query vector $x^\prime$ onto a codeword...
z_j’ e C_j. Then we do addition operation, i.e., \( x_i = d_i + z_j’ \). The \( i \) th component \( z_i \) can be recovered if and only if \(-\lambda_i / 2 < x_i - z_i < \lambda_i / 2\), and we finally get a matched pair of feature vectors. Hence, the distance projection can handle Gaussian errors falling into the range bounded by quantization steps.

### III. THE PROPOSED SCHEME FOR FINGERPRINT TEMPLATE PROTECTION

In this paper, we propose a scheme for fingerprint template protection based on distance projection. We use location and orientation information of a minutia as the coordinate feature \( m = (u, v, \theta) \). Given a fingerprint image \( I \) of size \( W_i \times H_i \), the minutiae set \( M = \{ m_i \}_{i=1}^{N} \) is extracted by VeriFinger 6.1 SDK [7], where \( N \) is the number of minutiae in \( I \). It is reported that VeriFinger SDK can obtain location and orientation information of a minutia exactly and avoid extraction of many spurious minutiae to assure good authentication performance. Note that VeriFinger 6.1 SDK has compacted the orientation scale from \([0,360]\) to \([0,255]\), we can specify the location and orientation scales of a minutia, i.e., \( 1 \leq u \leq W_i, 1 \leq v \leq H_i \) and \( 0 \leq \theta \leq 255 \).

#### A. Enrollment

At the enrollment stage, as illustrated in Figure 1, each minutia of the template image is processed by distance projection encoding procedure and secure hashing. Then a secured fingerprint template is generated by the concatenation of a random string, the difference vector and message digest of each minutia of the template fingerprint image. Given a minutia \( m = (u, v, \theta) \), the enrollment operates as follows:

1) **Initialization**: Choosing parameters \( \lambda = (\lambda_u, \lambda_v, \lambda_\theta) \) to obtain a codeword space by (1). Details of the quantization step selection are illustrated in section 4.

2) **Distance projection encoding**: Taking \( m \) as input of the encoding procedure of distance projection. The procedure outputs the difference vector \( d = (d_u, d_v, d_\theta) \) and the codeword vector \( z = (z_u, z_v, z_\theta) \). Only \( d \) is stored in the secured biometric template, while \( z \) considered as a secret.

3) **Secure hashing**: Selecting a random string \( r \) with specified length and concatenating it with the decoded feature vector \( m'' = (u'', v'', \theta'') \). Compute the hash value of the concatenated vector by \( h = \text{Hash}(r u v \theta) \), where \( \text{Hash} (\cdot) \) is any hash function such as SHA512, SHA256, MD5, etc. Then the hash value is stored in the template following the difference vector \( d \).

#### B. Verification

At the verification stage, as illustrated in Figure 2, each minutia of the query image is processed by distance projection decoding procedure and secure hashing check. Then a certain number of minutiae can be recovered. The query fingerprint image cannot be matched with the template image successfully until the number of recovered minutiae is greater than or equal to a predetermined threshold \( \text{num} \). Given a minutia \( m'' = (u'', v'', \theta'') \) and the secured template \( T \), the verification operates as follows:

1) **Initialization**: Using the same quantization parameters \( \lambda = (\lambda_u, \lambda_v, \lambda_\theta) \) as the enrollment stage to obtain a codeword space by (1).

2) **Distance-projection decoding**: Taking \( m'' \) as input of the encoding procedure of distance projection. The procedure outputs the query codeword vector \( z'' = (z_u', z_v', z_\theta') \). Do the addition operation of the difference vector \( d \) in the secured template and the codeword vector \( z'' \), i.e., \( m''_i = d_i + z''_i, 1 \leq i \leq t \).

3) **Secure hashing check**: Selecting a random string \( r' \) with specified length and concatenating it with the decoded feature vector \( m''_i = (u'', v'', \theta'') \). Compute the hash value of the concatenated vector by \( h' = \text{Hash}(r' u' v' \theta') \), and compare with \( h = \text{Hash}(r u v \theta) \), if \( h' = h \), the minutia is recovered, otherwise go step 2).

After processing the whole minutiae set \( M'' = \{ m''_i \}_{i=1}^{N} \) of the query image, we obtain the total number of recovered minutiae, i.e., \( \text{num}_\text{rec} \). And if the number is greater than or equal to a predetermined threshold \( \text{num} \), the query image can be considered as matched with the template image.
IV. EXPERIMENTAL RESULTS

The proposed fingerprint template protection scheme is evaluated on database FVC2002 DB2 [8], which contains 800 fingerprint images (100 × 8, 8 images per finger). All the images of DB2 are captured by the optical sensor “FX2000” by Biometrika, with resolution of 569 dpi and image size of 296 × 560.

A. Quantization step

The quantization step vector \( \lambda = (\lambda_u, \lambda_v, \lambda_\theta) \) has key effects on authentication performance and security of the system. Large quantization steps ensure high error tolerance ability, but result in false matches from different fingers as a side effect. Moreover, we will see that large quantization steps result in high entropy loss in section 5. A trade-off between system security and authentication accuracy should be carefully considered.

In our experiments, we select quantization parameters which satisfy the following condition [6]

\[
D_{m_1, m_2}(m_i, m_j) = \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2 + \beta_m|\Delta \theta_i - \Delta \theta_j|},
\]

where \( D_{m_1, m_2}(m_i, m_j) \) denotes the distance between two minutiae \( m_i \) and \( m_j \), and \( \beta_m \) is the weight assigned to the orientation component (set to 0.2). And we set \( \lambda_u = 2|u_i - u_j| \), \( \lambda_v = 2|v_i - v_j| \), \( \lambda_\theta = 2|\theta_i - \theta_j| \). Selection of well-separated minutiae ensures that they are assigned unique codewords when they are encoded into the codeword space \( C \). In our experiments, \( D_{m_1, m_2}(m_i, m_j) \) is set to no more than 25 as the maximum distance between a matched pair of minutiae. For instance, \( \lambda = (30, 32, 30) \) satisfies all the above conditions.

B. Numerical results

The criteria that are used for evaluating the performance are genuine accept rate (GAR) and false accept rate (FAR). The genuine accept rate is the percentage of attempts made by genuine users that resulted in successful authentication. The false accept rate is the percentage of attempts made by imposters that resulted in successful template recovery. Only impressions 1 and 2 of each finger in DB2 are used, so the number of genuine attempts is 100. The impostor attempts are simulated by trying to decode a user’s protected template using images from all the other users. Hence, the number of impostor attempts is 9900.

Due to fingerprint distortion, all pairings of minutiae between impressions 1 and 2 are pre-aligned in our experiments by the following external operation

\[
\begin{pmatrix}
\begin{pmatrix}
(\cos(\Delta \theta_1) - \sin(\Delta \theta_1) \Delta u) \\
\sin(\Delta \theta_1) \cos(\Delta \theta_1) \Delta v
\end{pmatrix} \\
1
\end{pmatrix} \begin{pmatrix}
1
\end{pmatrix} \theta^{(1)} = \theta^{(1)} + \Delta \theta,
\]

where \( (\Delta u, \Delta v, \Delta \theta) \) is the translation and rotation parameter vector, and \( (\theta^{(1)}, \theta^{(2)}, \theta^{(3)}) \) is the aligned coordinate feature vector of a minutia in impression 1.

Our experimental results under different quantization step vector \( \lambda = (\lambda_u, \lambda_v, \lambda_\theta) \) are shown in Table I. And the results of performance comparison between the proposed algorithm and fuzzy vault based method [6] are shown in Table 2. When \( \lambda = (22, 22, 28) \) and \( num = 13 \), the proposed scheme gains good authentication accuracy (GAR=92% vs. 86%, when FAR=0), and also high security (\( num = 13 \) vs. 11).

<table>
<thead>
<tr>
<th>( \lambda_u, \lambda_v, \lambda_\theta )</th>
<th>GAR(%)</th>
<th>FAR(%)</th>
<th>num</th>
</tr>
</thead>
<tbody>
<tr>
<td>(22, 22, 30)</td>
<td>89%</td>
<td>0</td>
<td>14</td>
</tr>
<tr>
<td>(22, 22, 28)</td>
<td>92%</td>
<td>0</td>
<td>13</td>
</tr>
<tr>
<td>(22, 22, 26)</td>
<td>86%</td>
<td>0</td>
<td>14</td>
</tr>
<tr>
<td>(22, 22, 24)</td>
<td>91%</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>(22, 22, 22)</td>
<td>86%</td>
<td>0</td>
<td>14</td>
</tr>
</tbody>
</table>

TABLE II. PERFORMANCE COMPARISON BETWEEN THE PROPOSED METHOD (\( \lambda = (22, 22, 28) \)) AND THE FUZZY VAULT METHOD ON FVC2002 DB2

<table>
<thead>
<tr>
<th>num</th>
<th>GAR(%)</th>
<th>11</th>
<th>12</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nandanakumar et al. [6]</td>
<td>GAR(%)</td>
<td>86%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proposed</td>
<td>GAR(%)</td>
<td>95%</td>
<td>94%</td>
<td>92%</td>
</tr>
<tr>
<td></td>
<td>FAR(%)</td>
<td>0.08%</td>
<td>0.02%</td>
<td>0</td>
</tr>
</tbody>
</table>

V. SECURITY ANALYSIS

The security of the proposed scheme is mainly based on the data stored in the secured template; the difference vector \( d \) and the feature hash value \( h = Hash(r || u || v || \theta) \). For a given codeword space \( C \) with parameters \( K \) and \( \lambda \), the entropy of \( m \) after observing \( d \) [9] is

\[
H(m|d) = H(m) - H(m_\text{eff}),
\]

where \( m_\text{eff} = m - z \). An upper bound of the mutual information \( H(m_\text{eff}) \) can be decided by

\[
H(m_\text{eff}) \leq \sum_{i=1}^{L} \log_2 \lambda_i.
\]

The feature hash value \( h \) also gives attackers a chance of brute force attack on a minutia one by one until \( num \). Based on the probability density functions \( f_u(v) \), \( f_v(v) \) and \( f_\theta(\theta) \), the maximum probability to guess a close minutia is

\[
p_m = \max_{u_i} \left( \sum_{u=\lambda_u/2}^{u_i/2} f_u(u) \right) \times \max_{v_i} \left( \sum_{v=\lambda_v/2}^{v_i/2} f_v(v) \right) \times \max_{\theta_i} \left( \sum_{\theta=\lambda_\theta/2}^{\theta_i/2} f_\theta(\theta) \right).
\]
Then the entropy of a template minutia under brute force attack is

\[ H(m | h) = - \log \sum p_m. \]  

When \( \lambda = (22, 22, 28) \) and \( num = 13 \), the system entropy is about 71 bits.

VI. CONCLUSION

Biometric template protection is essential for security of biometric authentication system and has aroused research highlights recently. A representative method is fingerprint template protection using the idea of the fuzzy vault, which still suffers security vulnerabilities and information leakage. In this paper, we design a codebook named distance projection for biometric coding to generate secured biometric template and propose a novel fingerprint template protection scheme to solve security limitation problems of the fuzzy vault-based method. Experimental results on FVC2002 DB2 show that the proposed scheme can obtain positive results on both security and authentication accuracy. Finally, our future work will concentrate on combining the proposed fingerprint template protection scheme with methods for removing burst errors to construct a minutia-based key binding system.

ACKNOWLEDGMENT

This paper is supported by the Project of National Natural Science Foundation of China under Grant No. 60875018 and 60621001, National High Technology Research and Development Program of China under Grant No. 2008AA01Z411, Chinese Academy of Sciences Hundred Talents Program, Beijing Natural Science Foundation under Grant No. 4091004, Scientific Databases Program of the Chinese Academy of Sciences during the 11th Five-Year Plan Period under Grant No. INFO-115-C01-SDB4-30.

REFERENCES