ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20220302094719
Original scientific paper

A Novel Fingerprint Encryption Based on Image and Feature Mosaic

Bing ZHENG, Zhenyu QIU*, Jing YANG

Abstract: Mobile smart devices in the digital era are enhancing personal information security by adopting fingerprint encryption technology, but due to the small size of mobile smart devices, the area of fingerprint image that can be detected is reduced, resulting in the lack of extractable fingerprint feature information, and traditional fingerprint encryption technology is difficult to apply to small area fingerprint images. To solve the application difficulties of small area fingerprint image encryption, a novel small area fingerprint encryption algorithm based on feature and image mosaic was proposed, and the encryption efficiency of the algorithm was verified using FVC2002 and XDFinger database. Results show that the small area fingerprint recognition algorithm based on feature and image mosaic is significantly improved in encryption efficiency, failure capture rate decreases from 36% to 7%, true acceptance rate increases from 44% to 68%, and the feasibility and reliability of the method is verified. Conclusions can promote the application of small area fingerprint encryption technology in mobile smart devices.

Keywords: feature mosaic; fingerprint encryption; image mosaic; small area

1 INTRODUCTION

Biometric technology is to achieve the purpose of identity authentication by statistical analysis of individual biological characteristics. Fingerprint identification technology has become one of the most mature and popular biometric authentication technologies due to its outstanding advantages of stability, personalization and high-cost performance.

Fingerprint encryption technology is the combination of fingerprint identification technology and information security technology [1-2]. It makes use of fingerprint features to achieve the purpose of binding personal identity information and key information. However, the fingerprint image area collected by the mobile intelligent device is greatly reduced, which directly leads to the lack of fingerprint feature information that can be extracted and used, so it is difficult to directly apply the traditional fingerprint encryption algorithms to small area fingerprint image [3-5].

The key problem of small area fingerprint image encryption technology is that there are not enough details for encryption and the matching of encryption domain is difficult. Small area fingerprint mosaic can fundamentally solve the problem that there is not enough matching detail feature set for small area fingerprint encryption algorithm due to insufficient fingerprint area [6]. Small area fingerprint image mosaic is achieved by iterative nearest point algorithm. Small area fingerprint mosaic can be divided into two directions: feature mosaic and image mosaic. Fingerprint image mosaic is to connect multiple fingerprint images of the same finger to form a fingerprint image with a large enough area. The feature information is obtained from the stitched fingerprint image, and then it can be used for the fingerprint encryption algorithm. Fingerprint feature mosaic is to put together the feature information of multiple fingerprint images of the same finger into a large set of feature points, and then use the stitched feature information to fingerprint encryption algorithm.

The rest of this study is organized as follows. Section 2 reviews the studies on fingerprint encryption technology. Section 3 introduces small area fingerprint encryption method based on feature mosaic and image mosaic. Section 4 verifies the proposed algorithm through experiments and analyses the experimental results. Section 5 draws conclusions.

2 STATE OF THE ART

Fingerprint encryption technology can significantly improve personal security and privacy, and it can solve the problems of memory inconvenience and easy loss in the key protection scheme. At present, fingerprint encryption system based on minutiae features can be divided into two types. One is fingerprint encryption system based on traditional minutiae matching algorithm, it needs to be aligned before matching. Another is the fingerprint encryption system without alignment. Traditional matching algorithm takes Cartesian coordinates [7] and directions of minutiae as matching features, which makes alignment an essential process. Juels et al. [8] proposed fuzzy vault algorithm, which effectively mediates the conflict between the accuracy of cryptography technology and the fuzziness of biometric authentication, and implements a practical key binding algorithm model. Fuzzy vault algorithm and fuzzy commitment algorithm [9] are the two most widely used biometric encryption algorithms. Many scholars have made different improvements on the basis of these two algorithms. Li et al. [10] extracted fixed-length binary vector as feature input through fingerprint triplet feature structure, combined with error correction code technology, fuzzy commitment algorithm is used to encrypt the fixed-length binary string extracted from fingerprint template. Yang et al. [11] used the improved Tyson polygon feature structure to extract the location and direction information as the fixed feature of fingerprint, and used the Pin Sketch algorithm model to encrypt. The scheme has better accuracy and higher security performance than the triplet feature structure. Mahmod et al. [12] proposed to extract the location and direction information of the global detail points as fixed features by constructing polar coordinate system and protecting the original information of fingerprint template by irreversible transformation of the extracted feature information. The above methods have achieved some results in the conventional area fingerprint, but because the small area fingerprint image is limited by

the lack of feature information, the length of the key that can be bound is short, so the above methods cannot be directly applied to the small area fingerprint encryption.

Small area fingerprint mosaic technology is used to solve the insufficient information problem of a single small area fingerprint [13]. Through the registration of multiple small area fingerprint images or feature templates of a finger, a large area fingerprint image or feature template with more information is formed. He et al. [14] studied reflection transformation, projection transformation and topological transformation, and spliced the minutiae in fingerprint image. The algorithm improved the fingerprint recognition accuracy and reduced the computational complexity. Bhuvaneshwari et al. [15] proposed an improved iterative closest point algorithm to calculate the transformation matrix of the spatial position relationship of two images, and then stitched the fingerprint images. Bian et al. [16] added ridge information to fingerprint mosaic, the two stitched fingerprint images are further aligned according to the ridge matching error after obtaining the distance image, and it effectively improved the recognition accuracy. Hirohata et al. [17] proposed to use the TPS model to build the elastic distortion of the spliced image. The scheme found the initial correspondence by matching and connecting to the matching minutiae and ridgeline and then used the TPS model for accurate registration. Choi et al. [18] proposed a recursive ridge mapping method to reduce the matching error of the image, and stitched five small area images of the same finger and achieved good results. Tong et al. [19] used the improved phase correlation method to calculate the image translation parameters for the alignment process. The algorithm reduced the computational complexity and improved the system's robustness.

3 METHODOLOGY

3.1 Small Area Fingerprint Encryption Method Based on Feature Mosaic

The key problem of small area encryption technology is that there are not enough details for encryption and the matching of encryption domain is difficult. Fingerprint feature mosaic is to piece together the feature information of multiple fingerprint images of the same finger into a large set of feature points, and then use the stitched feature information to fingerprint encryption algorithm. The flow of small area fingerprint encryption algorithm based on feature mosaic is shown in Fig. 1.

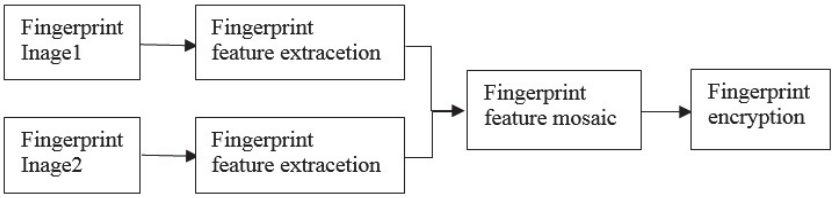

Figure 1 The flow of small area fingerprint encryption algorithm based on feature mosaic

In this study, rigid transform is used as the coordinate transformation model of fingerprint feature mosaic. Direction field operators with relative detail features are added to determine the minutiae pairs for estimating rigid body transformation. Feature mosaic makes full use of fingerprint minutiae feature information and direction field descriptor information, effectively solving the problem that the traditional fingerprint fuzzy vault algorithm cannot be used due to the small area of fingerprint image and the small number of fingerprint minutiae. The advantage of the design is that it increases the total number of real minutiae, reduces the failure rate of system acquisition, improves the correct acceptance rate of the encryption system, and ensures the safety strength of the encryption system.

3.1.1 Extraction of Fingerprint Feature Points

In this study, the ridge contour of fingerprint is detected by traversing the binary image of fingerprint from top to bottom and from left to right. Then the ridge contour is tracked counter-clockwise and expressed as a matrix of contour elements. All the element information of the ridgeline is recorded in a matrix. According to the information recorded by the matrix, the minutiae of the fingerprint can be obtained. Each contour element represents a pixel on the contour, which includes auxiliary information such as coordinate values of the pixel, angular values of the contour, curvature, etc. In the fingerprint binarization image, the ridgeline spans more than one pixel and tracks the ridgeline along its contour counter-clockwise. When the trajectory is significantly leftward, the endpoint will be detected. Similarly, when the trajectory is obviously to the right, the bifurcation point will be detected.

The incident vector and the exit vector of the point o are respectively defined as o_{in}, o_{out}. And they are calculated by the points on the adjacent contour around the point o. It is to prevent some noise and obtain a more accurate estimation phasor by using the mean value of more than one point. The change value θ of ridge line direction of point o depends on the angle between o_{in} and o_{out}, as shown in Eq. (1).

$$\theta = \arccos \frac{o_{\text{in}} \cdot o_{\text{out}}}{|o_{\text{in}}||o_{\text{out}}|} \tag{1}$$

where, $o_{\text{in}} \cdot o_{\text{out}}$ is the dot product of two vectors, $|o_{\text{in}}||o_{\text{out}}|$ is the product of the modules of two vectors and $arccos$ is the inverse cosine function.

The two vectors are normalized to $o_{\text{in}} = (a_1, b_1)$, $o_{\text{out}} = (a_2, b_2)$ respectively, then the size of θ can be determined by Eq. (2).

$$\theta = \arccos(a_1 a_2 + b_1 b_2) \tag{2}$$

The threshold value T is set to count the case where any obvious deflection conforms to Eq. (4), and any point conforming to Eq. (3) is considered as a minutia point:

$$a_1a_2 + b_1b_2 < T \tag{3}$$

The two vectors are transformed into the Cartesian coordinate system. If o_{in} follows the axis, the threshold T is defined as a line perpendicular to the abscissa axis. Since the θ is in the range of −90° to 90°, the angle difference between the two vectors can be expressed by sinθ, as shown in Eq. (4).

$$\sin\theta = a_1b_2 - a_2b_1 \tag{4}$$

where, $a_1b_2 - a_2b_1 > 0$ represents the left turn, $a_1b_2 - a_2b_1 < 0$ represents the right turn, $a_1b_2 - a_2b_1 = 0$ represents no deflection. After the above steps, the minutiae feature $F = \left\{F_i\left(a_i, b_i, \theta_i\right)\right\}_i^n = 1$ of the fingerprint is completely detected, where n is the number of minutiae.

There are many types of fingerprint feature descriptors. In this study, a single detail feature a is taken as a representative to illustrate the structure of its relative directional field descriptors.

The detail feature a is taken as the circle center, M concentric circles with radius r_l are constructed, and N_m sampling points $o_{n,m}$ are selected on each circle, where m and n need to satisfy $1 < m < M$ and $1 < n < N_m$. The Tico descriptor corresponding to this minutiae point is constructed as shown in Eq. (5):

$$O(a) = \left\{\left\{\lambda\left(\theta_{n,m}, \theta\right)\right\}_{n=1}^{N_m}\right\}_{m=1}^{M} \tag{5}$$

where, $\theta_{n,m}$ is the direction field value of the sampling point $\theta_{n,m}$, $\lambda(\theta_{n,m}, \theta)$ represents the direction field value of the sampling point $\theta_{n,m}$ with respect to the minutiae a, $O(a)$ is the minimum direction field difference value that the sampling point direction field moves counter-clockwise to be parallel to the minutiae direction field.

3.1.2 Fingerprint Feature Mosaic

Matching two specified feature templates through fingerprint features is a key step, and it is also necessary to find a transformation model F for the specified two feature templates T_A and T_B, so as to minimize Eq. (6).

$$\left\|F\left(T_A\right) - T_B\right\| \tag{6}$$

where, $F(T_A)$ is the transformed feature template and $\|\cdot\|$ is the 2-norm.

$\left\|F\left(T_A\right) - T_B\right\|$ is the distance between the transformed feature template and the original feature template. The lower the $\left\|F\left(T_A\right) - T_B\right\|$ between the two splicing templates, the better the similarity, the higher the correctness of the model F. After determining the spatial position relation corresponding to the two splicing templates, the position transformation operation is carried out, and aligning one splicing template with the other splicing template as a reference template by using a transformation model F. The two mosaic templates can be integrated to obtain fingerprint feature mosaic only when the coordinate angles and the like are transformed into the same spatial relation through the transformation model F. Thus coordinate transformation is very necessary. The fingerprint database used in this study has rotated and translated the collected data, and the fingerprint image is small and the number of minutiae is relatively small. Therefore, the rigid transform is selected as the transformation model to correct the fingerprint feature mosaic.

Rigid transformation refers to the coordinates in the image being only translated and rotated while the relative positions remain consistent, as shown in Fig. 2. The relative position between the two points of the image is consistent after the rigid transformation, and the relative spatial relationship such as parallel and vertical is maintained.

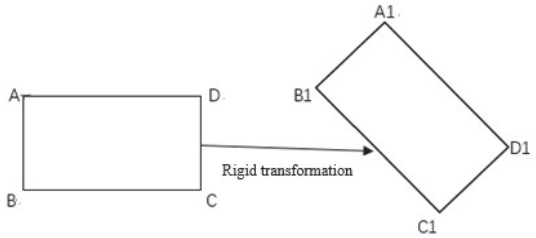

Figure 2 Schematic diagram of rigid transformation

In this study, the rigid transformation is selected as the transformation model, and then the parameters of the rigid transformation model need to be determined. The transformation parameters are estimated by using minutiae pairs, and Tico descriptors of minutiae are extracted. The similarity of any two Tico descriptors of minutiae between two feature templates is calculated, and the probability between any two minutiae point is calculated according to the similarity between Tico descriptors. If the similarity between two minutiae is high and the similarity with other minutiae is low, the probability value is high. The transformation parameter is calculated by selecting the minutiae pair with the highest probability.

Minutiae s and t are taken as examples, the process of calculating the matching probability between their corresponding Tico descriptors $O(s) = \{s_{n,m}\}$ and $O(t) = \{t_{n,m}\}$.

The first step is to calculate the directional field difference between all sampling points according to Eq. (7):

$$s_{n,m} = \Lambda\left(s_{n,m}, t_{n,m}\right) = \left(2/\pi\right)\min\left(s_{n,m}, t_{n,m}\right), \lambda\left(t_{n,m}, s_{n,m}\right) \tag{7}$$

where, $\Lambda(s,t)$ is the directional distance between s and t, and when $\Lambda(s,t)$ is 0, the directional spatial relationship between the center point and the sampling point is parallel.

When the value of $\Lambda(s,t)$ is 1, it means that the directional spatial relationship between the center point and the sampling point is vertical.

The second step is to calculate the similarity between s and t according to Eq. (8):

$$Sim(s,t)=\left(\frac{1}{N}\right)\sum_{m=1}^{M}\sum_{n=1}^{N_m}\mathrm{s}\left(a_{n,m}\right) \tag{8}$$

where, $Sim(s, t)$ is the similarity between s and t, $s(x)$ represents the similarity of the difference x between the two direction fields.

Then according to Eq. (9), the probability between s and t can be solved:

$$P(s,t)=\frac{Sim(s,t)^2}{\left[\sum_{i'}^{N}S(s_{i'},t)+\sum_{j'}^{N}S(s,t_{j'})-Sim(s,t)\right]} \tag{9}$$

After obtaining the minutiae pairs of estimated transformation parameters, in this study, the following pairs of minutiae are first assumed to be selected: $\{(a_1,b_1),(a_2,b_2)\},\ldots,(a_N,b_N)$, then the rotation and translation parameters corresponding to each matched pair of minutiae points can be obtained according to $\mathrm{d}x=x_a-x_b$, $\mathrm{d}y=y_a-y_b$, $\mathrm{d}\theta=\theta_a-\theta_b$. According to Eq. (6), the feature points in the feature template T_A are transformed to the coordinate system where the feature template T_B is located through rigid transformation. The Tico descriptor is unchanged, and the transformed feature template is set to T_A'. In the probability matrix, the probability between the minutiae pairs satisfying T_A' and T_B in Eq. (10) is set to 0:

$$\left|x_a'-x_b\right|>thr_x\cup\left|y_a'-y_b\right|>thr_y\cup\left|\theta_a'-\theta_b\right|>thr_\theta \tag{10}$$

where, thr_x, thr_y, thr_θ are the thresholds of coordinates and angles of minutiae pairs.

According to the rotation and translation parameters, the greedy algorithm is used to obtain the matching minutiae pairs in this study, and the Euclidean distances of the matching minutiae pairs are summed. In this way, each matching minutiae pair corresponds to a Euclidean distance sum, and the optimal rotation and translation parameter is defined as the rotation and translation parameter corresponding to the sum of the minimum Euclidean distances.

According to the optimal rotation and translation parameters of the two feature templates T_A and T_B, the point pairs in the template T_A' registered with the template T_B are obtained, and feature splicing is preliminarily completed. But the existing feature splicing template has overlapping features. Then we need to deal with the minutiae pairs in the overlapping area. For coincident matching minutiae pairs, the average value of minutiae pairs is calculated as a new minutiae point to replace the original minutiae pair.

Assuming that (a_1, b_1) is a coincident minutiae pair, and a_1 is transformed to the splice template a_1' through rigid transformation, minutiae a_1' and b_1 are deleted from the splice feature template to generate new minutiae b_{new}, and the coordinates and directions of the new minutiae are obtained from Eq. (11):

$$\begin{cases} b_{\text{new}}\cdot x=\dfrac{a_1'\cdot x+b_1\cdot x}{2} \\ b_{\text{new}}\cdot y=\dfrac{a_1'\cdot y+b_1\cdot y}{2} \\ b_{\text{new}}\cdot \theta=\dfrac{a_1'\cdot \theta+b_1\cdot \theta}{2} \end{cases} \tag{11}$$

where, $b_{\text{new}}\cdot x$, $b_{\text{new}}\cdot y$ and $b_{\text{new}}\cdot\theta$ are the abscissa, ordinate and angle of the new minutiae, respectively.

3.1.3 Encryption Method

The obtained minutiae template and the Tico descriptor corresponding to the minutiae are used for encryption. The encryption method is the process of binding the key and fingerprint minutiae and generating an encryption algorithm, as shown in Fig. 3.

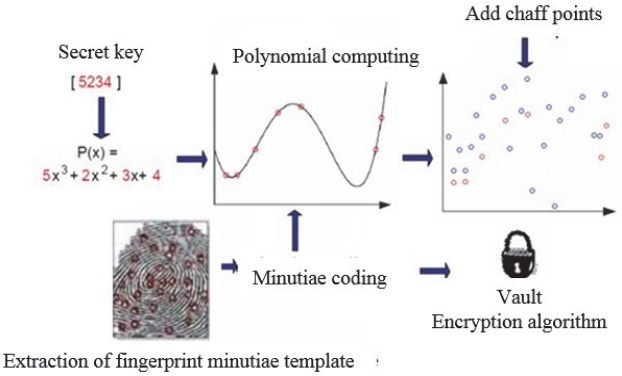

Figure 3 Flow chart of the encryption method

The processing of minutiae mainly includes two parts: minutiae screening and minutiae coding. Its purpose is to make encryption more accurate and convenient for subsequent polynomial calculation.

The principle of selecting minutiae is to select some minutiae that are well separated from the set of minutiae. The usual selection method is the threshold method. When the minimum distance between two minutiae points is greater than a given threshold, the two minutiae points have good distinguishability. The distance function of two minutiae points p_i, p_j is D_m, and the calculation is shown in Eq. (12):

$$D_m\left(p_i,p_j\right)=\sqrt{\left(x_i-x_j\right)^2+\left(y_i-y_j\right)^2}+\delta_M\Delta\left(\theta_i,\theta_j\right) \tag{12}$$

where, $\Delta\left(\theta_i,\theta_j\right)=\min\left(\left|\theta_i-\theta_j\right|,360-\left|\theta_i-\theta_j\right|\right)$ represents the difference between the two angles, x and y represent the abscissa and ordinate of the minutiae respectively, θ represents the angle of the minutiae and δ_M is the weight assigned to the angle.

Minutiae information represented by a three-dimensional vector (x, y, θ) is converted into a 16-bit string by the minutiae encoding. According to the size $H \times W$ of the input image, x, y, θ are converted into 6 bits, 5 bits and 5 bits in sequence, and the conversion method is shown in Eq. (13).

$$\begin{cases} x' = x \cdot 2^6 / W \\ y' = y \cdot 2^5 / H \\ \theta' = \theta \cdot 2^5 / 360 \end{cases} \tag{13}$$

(x', y', θ') is sequentially converted into binary string $Bx, By, B\theta$ and concatenated into a 16-bit string $X = Bx \| By \| B\theta$, and the minutiae coding is completed.

The purpose of adding chaff points is to protect real minutiae and ensure the security of fingerprint encryption algorithm. The chaff point is added as follows:

The fingerprint image is divided into several segments, called image units, and unique chaff points are randomly generated in the image units. It is noticed that each image unit has 8 adjacent image units. A new chaff point c is randomly generated according to the following two criteria: (1) a unique chaff point is randomly generated in any image unit. If the image unit already contains real minutiae or chaff point, the image unit is ignored; (2) the distance between this new point and the existing 8 points is large or equal to δ.

Each feature point in the encryption point set is matched with a polynomial operation result $P(X)$ and a Tico descriptor. Chaff point c should also be matched with a pseudo-operation result f and a pseudo-Tico descriptor to confuse the real encryption point and chaff point. For pseudo-operation result f, the random addition method can ensure that it is not repeated with the polynomial operation result of the real minutiae. For pseudo-Tico descriptors, the adopted method in this study is to select a texture image with a size of $H \times W$ and independent of fingerprints, extract the direction field information of the texture image, and obtain the pseudo-Tico descriptor corresponding to chaff point c on the image. Until enough chaff points are generated, the chaff point set c and the set G are merged, the order is disordered, the Tico descriptors are stored, and the final encryption algorithm is generated.

3.2 Small Area Fingerprint Encryption Method Based on Image Mosaic

Fingerprint image mosaic is to connect multiple fingerprint images of the same finger to form a fingerprint image with a large enough area, obtain the feature information from the stitched fingerprint image, and then use the feature information to the fingerprint encryption algorithm. The flowchart of small area fingerprint encryption algorithm based on image mosaic is shown in Fig. 4.

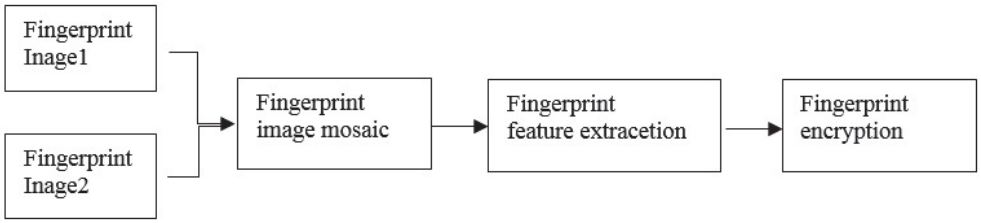

Figure 4 The flow of small area fingerprint encryption algorithm based on image mosaic

3.2.1 Fingerprint Image Mosaic

Initial reference point selection is crucial to the accuracy of fingerprint image mosaic. In the iterative closest point algorithm (ICP) used for fingerprint image mosaic, the determination of initial reference points includes two types of methods: (1) all the minutiae pairs in the two minutiae sets are scanned, the number of minutiae feature pairs on which the transformation parameters corresponding to each pair of combinations can match is counted, and the most numerous minutiae pair combinations are set as initial reference points. (2) The fingerprint center point is set directly as the initial reference point. However, both of these two methods have defects: the first one is not only complicated in operation and wastes a lot of resources and time, but also has low accuracy in determining reference points only according to the number of matching detail features. The other does not apply to images that do not include center points.

In view of the above defects, the matching detail feature pair with the highest similarity is set as the reference point. It not only simplifies the calculation and saves time, but also avoids the situation that reference points cannot be selected without center points. In this study, the method described in reference is used to carry out minutiae-based matching algorithm on fingerprint images to obtain matching minutiae pairs.

In this study, reference points are selected to calculate the initial transformation parameters at the same time. To reduce the registration error of image mosaic, the initial transformation parameters are optimized in this study. The optimization condition of iterative closest point algorithm in fingerprint image mosaic is the sum of squares of Euclidean distances between two minutiae sets, which only uses minutiae information and does not use ridge features of fingerprints. In this study, the registration error of the normalized distance map is calculated as an optimization index to determine the estimation accuracy of transformation.

The gray value of the pixel point in the refined image is set by the distance map as the Euclidean distance between the point located on the ridgeline closest to the pixel point, and the distance image Q_D can be represented by Eq. (14) through the refined image Q_T. The distance image is shown in Fig. 5.

$$Q_D(x,y) = \min\left\| r_n^Q - Q_T(x,y) \right\| \quad (14)$$

where $r_n^Q \in R^Q = \left\{ r_1^Q, ..., r_n^Q, ..., r_{N_q}^Q \right\}$, represents the point set on the ridge line in the refined image Q_T.

Figure 5 The distance map of fingerprint image

The initial transformation parameters of the fingerprint images *A* and *B* are calculated by using the initial reference points and coordinate transformation is carried out to transform the ridge points of A_T in the coincidence area between the refined image A_T and the distance image Q_D to the coordinate system B_T. If the rotation and translation parameters are good, the ridge points of A_T in the coincidence area are converted to B_T and still be on the ridge line, which indicates that the gray value that A_T projected on the distance image Q_D is small and the ridge matching error (*RME*) of A_T and Q_D is small. The ridge matching error can be calculated according to Eq. (15).

$$RME = 1 / N_{AB} \sum_{K=1}^{N_{AB}} Q_D\left(X'(i,j,\theta), Y'(i,j,\theta) \right) \quad (15)$$

where, N_{AB} represents the number of r_m^a, r_m^a represents the number of ridge points of A_T in the overlapping area between the refined image A_T and the distance image Q_D.

The optimal rotation and translation parameters $(\mathrm{d}x_0 + i, \mathrm{d}y_0 + j, \mathrm{d}\theta_0 + \theta)$ of image mosaic are defined as the rotation and translation parameters when the ridge matching error reaches the minimum value. According to the optimal transformation parameters, the coordinates of pixel points in fingerprint image *A* transformed into fingerprint image *B* can be determined to obtain the fingerprint mosaic image. The mosaic image is shown in Fig. 6.

Fingerprint image enhancement, binarization and other pre-process operations are sequentially carried out on spliced fingerprint images obtained by the user through fingerprint image mosaic. According to the fingerprint pre-processed image, the coordinate and direction of the fingerprint minutiae points are sequentially extracted from left to right and from top to bottom to generate a minutia point set $M = \left\{ M_i\left(x_i, y_i, \theta_i\right) \right\}_i^n = 1$, where *n* is the number of minutiae points, and direction field information is extracted. Using the direction field information of the spliced fingerprint image, Tico descriptors around the minutiae are extracted and stored in Helper Data.

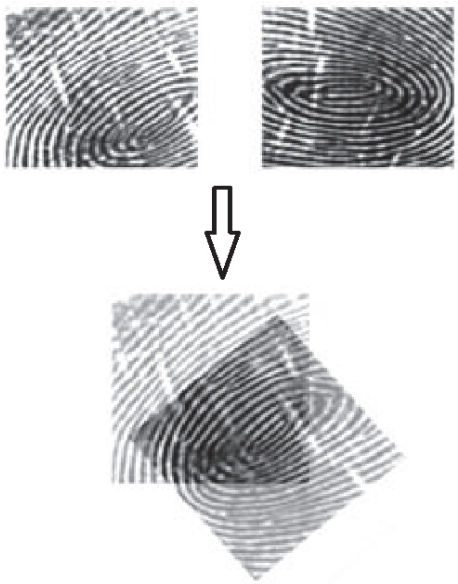

Figure 6 An example of fingerprint image mosaic

3.2.2 Encryption Domain Matching Policy

The principle of encryption domain matching is that fingerprint information used for encryption is not disclosed, so fingerprint minutiae cannot be directly used for registration. In this study, the minutiae feature information and Tico descriptor feature information of fingerprint are extracted and verified. The Tico descriptor is used for encryption domain matching. The matching process is described as follows: Firstly, the similarity of two Tico descriptors is calculated. Assuming that the minutiae points in the registered fingerprint and the verification fingerprint are *s* and *t* respectively, and the Tico descriptors corresponding to the minutiae points are $O(s) = \left\{ \mathrm{s}_{n,m} \right\}$ and $O(t) = \left\{ t_{n,m} \right\}$, then the similarity calculation of the two Tico descriptors can be performed by Eq. (16).

$$S(s,t) = \left(\frac{1}{k} \right) \sum_{m=1}^{M} \sum_{k=1}^{K_m} s\left(x_{n,m} \right) b \quad (16)$$

where, $K = \sum_{m=1}^{M} K_m$, $x_{n,m} = \Lambda\left(s_{n,m}, t_{n,m} \right)$, $s(x) = e^{-16x}$, represent the similarity between two direction fields with distance *x*, and $s(0) = 1$ represents the maximum similarity between the two directional fields.

A Tico descriptor of a decrypted fingerprint is constructed, and a Tico descriptor of a registered fingerprint from a vault is extracted, scanning the Tico descriptors of all detail feature pairs of the decrypted fingerprint and the registered fingerprint, then the similarity of the Tico descriptors of all detail feature pairs is obtained according to a similarity calculation formula, selecting the top-N Tico descriptors with the highest similarity to calculate transformation control parameters, the coordinate transformation is carried out on the decrypting fingerprint detail features (x, y, θ) according to transformation comparison parameter, the detailed features of the decrypted fingerprint after transformation and the Euclidean distance of the midpoint in the vault are calculated, and the detailed feature pairs within the

Euclidean distance threshold range are judged to be correctly matched. Real minutiae are preserved in the form of matching feature pairs. When the decrypted fingerprint and the registered fingerprint belong to the same finger, several chaff points in the vault can be filtered out.

The points belonging to the vault in the matching detail feature pair to the decryption point set T are added. In this study, the Tico descriptor is transformed according to the N with the highest similarity, so N decryption point set will be obtained. In the following process, these N decryption point sets will be reconstructed by polynomial in turn.

For polynomial reconstruction, firstly, the number of detail features in the set T is determined. Only when the number is not lower than the highest order term of the construction polynomial, the polynomial can be reconstructed and the coefficients can be obtained by combining Lagrange polynomial interpolation method [20]. Otherwise, it is determined that decryption failed. The construction of Lagrange interpolation polynomial P' is shown in Eq. (17).

$$p(x)=\frac{(x-g_2)(x-g_3),...,(x-g_9)}{(g_1-g_2)(g_1-g_3),...,(g_1-g_9)}h_1+\frac{(x-g_1)(x-g_3),...,(x-g_9)}{(g_2-g_1)(g_2-g_3),...,(g_2-g_9)}h_2+...+\frac{(x-g_1)(x-g_2),...,(x-g_8)}{(g_9-g_1)(g_9-g_2),...,(g_9-g_8)}h_9 \quad (17)$$

A series of coefficients $r'_0, r'_1, ..., r'_t$ are calculated every time, the temporary key K' is generated by concatenation of' these coefficients. The MD5 function is used to hash K' to $MK'=h(K')$, and MK' is scanned cyclically to distinguish whether r'_t is one of its connected substrings with a unit of 16 bits. If it is consistent with one of the connected substrings of MK', then it is considered that the decryption process is successful, and the ciphertext vault is changed into plaintext K', otherwise, t points are taken out from the decryption point set T again and brought into the formula for solution, and the process is repeated until all combinations of all t points in T re-scanned and extracted again and still fail, then it is deemed that the ciphertext vault has not been successfully changed into plaintext.

3.3 Sample Data Selection

In experiment, FVC2002 DB1 [21] and XDFinger fingerprint databases [22] are used. Eight fingerprint images of 100 people are randomly selected for experiments. The top-7 images are used for splicing and encrypting different numbers of fingerprint images, and the last image is used for decryption. The size of the secret key is 128 bits.

4 RESULTS ANALYSIS

Failure capture rate (*FCR*), true acceptance rate (*TAR*) and false acceptance rate (*FAR*) are acted as criteria to evaluate performance. *FCR* represents the percentage of the number of failed fingerprints to the total number of fingerprints. *TAR* is defined as the percentage of real user attempts that resulted in successful authentication. *FAR* is defined as the percentage of attempts by impostors to successfully decode the vault corresponding to legitimate users. Attempts by impostors are simulated by decoding the user's vault using fingerprints from all other users. For FVC and XDFinger databases, the number of attempts made by impostors is 100 × 99 for 100 fingers. The experimental results are shown in Tab. 1.

In Tab. 1, XDFinger1 refers to fingerprint image mosaic based on XDFinger database; XDFinger2 refers to fingerprint feature mosaic based on XDFinger database, and the number in brackets refers to the number of small-area fingerprints for fingerprint mosaic.

Table 1 Results of small area fingerprint encryption algorithm based on image mosaic

Database	*FCR*	*TAR*	*FAR*
FVC2002 DB1	2%	90%	0.12%
XDFinger	36%	44%	0.02%
XDFinger1(3)	15%	57%	0%
XDFinger1(4)	12%	66%	0.01%
XDFinger1(5)	7%	68%	0.03%
XDFinger1(6)	7%	69%	0.05%
XDFinger1(7)	7%	69%	0.06%
XDFinger2(3)	14%	56%	0%
XDFinger2(4)	12%	58%	0.01%
XDFinger2(5)	11%	62%	0.09%
XDFinger2(6)	11%	60%	0.05%
XDFinger2(7)	10%	61%	0.07%

The experimental results are analysed as follows:

Firstly, a comparative experiment is made on the performance of conventional full fingerprint image and small area fingerprint image in fingerprint fuzzy vault algorithm. The negative influence of small area fingerprint image on fingerprint fuzzy vault algorithm is verified. As shown in Tab. 1, its *TAR* reaches 90%, but when directly applied to small area fingerprints, *FCR* has increased from 2% to 36% and *TAR* has decreased to 44%, which is obviously due to insufficient details for fingerprint encryption with good separability.

As can be seen from Tab. 1, the performance of the small area fingerprint encryption algorithm based on image mosaic is better than that of the small area fingerprint encryption algorithm based on feature mosaic in terms of *FCR* or *TAR* when the number of fingerprint mosaics is the same. Through the process analysis of the two algorithms, the alignment of minutiae points in overlapping areas is carried out by means of the direction field descriptor Tico during fingerprint feature mosaics. However, when Helper Data is stored, only Tico descriptors of one of the coincident minutiae points can be stored, resulting in errors in encryption domain matching, and the effect is not better than that of the small area fingerprint encryption algorithm based on image mosaic.

By comparing and analyzing the number of fingerprint mosaics, first of all, we can see that fingerprint mosaics have significantly improved the performance of small area fingerprint encryption algorithm. Compared with a single small area fingerprint image, when 5 fingerprint image mosaics are used for small area fingerprint encryption algorithm experiments, *FCR* decreases from 36% to 7%, *TAR* increases from 44% to 68%. Secondly, the more

fingerprint images used for splicing is not the better. When the number is 5, the performance of the small area fingerprint encryption algorithm tends to be stable, *FCR* will no longer decrease, and *TAR* will decrease slightly. After analysis, too many fingerprint images are used for splicing, which will lead to the increase of false details, thus negatively affecting the encryption algorithm.

5 CONCLUSION

In this study, the encrypted minutiae set was expanded by feature mosaics and image mosaics respectively. Firstly, the fingerprint feature mosaic algorithm based on the direction field descriptor and rigid transformation method was used to directly increase the number of minutiae while making full use of the encrypted domain matching descriptor. Then, the fingerprint image mosaic based on minutiae and distance images not only expands minutiae but also enriches other fingerprint features, which is beneficial to the utilization of various feature information in encrypted domain matching. Finally, the feasibility and reliability of the method in this study were verified by encryption domain matching experiments. The following conclusions can be drawn:

(1) A design scheme for a small area fingerprint encryption based on fingerprint mosaic was implemented. For the problem that the number of fingerprint feature information extracted is small, the fingerprint feature mosaic and fingerprint image mosaic are used to increase the fingerprint feature information effectively respectively.

(2) A fuzzy vault algorithm based on multiple feature descriptors is implemented to improve the similarity between matched detail point pairs for the problem of fingerprint encryption domain matching. Failure capture rate decreases from 36% to 7%, true acceptance rate increases from 44% to 68%. The performance of fingerprint encryption algorithm is significantly improved on small area fingerprints.

Future research needs to explore small area fingerprint encryption to meet the needs of a wider range of applications. For example, the pseudo-detail points generated by the fingerprint feature mosaic in this study still interfere with the extraction of feature information, and there is a need to implement accurate mosaic images for small area fingerprint encryption algorithms in the future.

Acknowledgements

This study is supported by the Teaching Reform Project of Hainan Education Department (No. HNJG2019-135).

6 REFERENCES

[1] Hashad, F. G., Zahran, O., El-Rabaie, E. S. M., Elashry, I. F., El-Samie, A., & Fathi, E. (2019). Fusion-based encryption scheme for cancelable fingerprint recognition. *Multimedia Tools and Applications*, *78*, 27351-27381. https://doi.org/10.1007/s11042-019-7580-x

[2] Lai, Q., Wan, Z., Akgul, A., Boyraz, O. F., & Yildiz, M. Z. (2020). Design and implementation of a new memristive chaotic system with application in touchless fingerprint encryption. *Chinese Journal of Physics*, *67*, 615-630. https://doi.org/10.1016/j.cjph.2020.08.018

[3] Kaur, J. & Jindal, N. (2019). A secure image encryption algorithm based on fractional transforms and scrambling in combination with multimodal biometric keys. *Multimedia Tools and Applications*, *78*, 11585-11606. https://doi.org/10.1007/s11042-018-6701-2

[4] Bisio, I., Garibotto, C., Lavagetto, F., & Sciarrone, A. (2021). Computational Complexity Closed-Form Upper Bounds Derivation for Fingerprint-Based Point-of-Interest Recognition Algorithms. *IEEE Transactions on Vehicular Technology*, *69*(8), 9083-9096. http://doi.org/10.1109/TVT.2020.3000568

[5] Liu, L., Hao, S., Lin, J., Wang, Z., Hu, X., & Miao, S. (2018). Image block encryption algorithm based on chaotic maps. *IET Signal Processing*, *12*(1), 22-30. https://doi.org/10.1049/iet-spr.2016.0584

[6] Su, Y., Xu, W., Li, T., Zhao, J., & Liu, S. (2021). Optical color image encryption based on fingerprint key and phase-shifting digital holography. *Optics and Lasers in Engineering*, *140*. https://doi.org/10.1016/j.optlaseng.2021.106550

[7] Bin, S. & Sun, G. (2020). Optimal energy resources allocation method of wireless sensor networks for intelligent railway systems. *Sensors*, *20*(2), 482. https://doi.org/10.3390/s20020482

[8] Juels, A. & Sudan, M. (2006). A fuzzy vault scheme. *Designs, Codes and Cryptography*, *38*(2), 237-257. https://doi.org/10.1007/s10623-005-6343-z

[9] Liu, Z., Li, Q., & Niu, X. (2013). Improve the security of image robust hash using fuzzy commitment scheme. *Neural Computing and Applications*, *23*(1), 67-72. https://doi.org/10.1007/s00521-012-0850-4

[10] Li, P., Yang, X., Qiao, H., Cao, K., Liu, E., & Tian, J. (2012). An effective biometric cryptosystem combining fingerprints with error correction codes. *Expert Systems with Applications*, *39*(7), 6562-6574. https://doi.org/10.1016/j.eswa.2011.12.048

[11] Yang, W., Hu, J., Wang, S., & Stojmenovic, M. (2014). An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures. *Pattern Recognition*, *47*(3), 1309-1320. https://doi.org/10.1016/j.patcog.2013.10.001

[12] Mahmod, S. M., Daud, S. M., Yuhaniz, S. S., Azizan, A., & Sjarif, N. N. A. (2017). Improving accuracy of decoding process with pore-based fingerprint fuzzy vault in biometric cryptosystem. *Advanced Science Letters*, *23*(5), 4068-4073. https://doi.org/10.1166/asl.2017.8339

[13] Kim, B. S. & Kim, T. G. (2019). Cooperation of simulation and data model for performance analysis of complex systems. *International Journal of Simulation Modelling*, *18*(4), 608-619. https://doi.org/10.2507/IJSIMM18(4)491

[14] Panahi, P., Bayilmis, C., Cavusoglu, U., & Kacar, S. (2021). Performance Evaluation of Lightweight Encryption Algorithms for IoT-Based Applications. *Arabian Journal for Science and Engineering*, *46*, 4015-4037. https://doi.org/10.1007/s13369-021-05358-4

[15] Bhuvaneshwari, B. & Rajeswari, A. (2018). 3D Reconstruction using artificial bee colony based iterative closest point algorithm. *Journal of Intelligent & Fuzzy Systems*, *35*(2), 1721-1732. http://doi.org/10.3233/JIFS-169708

[16] Bian, W., Ding, S., & Xue, Y. (2017). Fingerprint image super resolution using sparse representation with ridge pattern prior by classification coupled dictionaries. *IET Biometrics*, *6*(5), 342-350. https://doi.org/10.1049/iet-bmt.2016.0097

[17] Hirohata, M. (2016). Elastic mechanical behavior of spliced joints assembled by fillet welding and bonding. *Welding in the World*, *60*(2), 327-335. https://doi.org/10.1007/s40194-016-0298-8

[18] Choi, K., Choi, H., Lee, S., & Kim, J. (2007). Fingerprint image mosaicking by recursive ridge mapping. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *37*(5), 1191-1203. http://doi.org/10.1109/TSMCB.2007.907038

[19] Tong, X., Xu, Y., Ye, Z., Liu, S., Li, L., Xie, H., Wang, F. Gao, S., & Stilla, U. (2015). An improved phase correlation method based on 2-D plane fitting and the maximum kernel density estimator. *IEEE Geoscience and Remote Sensing Letters*, *12*(9), 1953-1957. https://doi.org/10.1109/LGRS.2015.2440340

[20] Sun, G. & Bin, S. (2018). A new opinion leaders detecting algorithm in multi-relationship online social networks. *Multimedia Tools and Applications*, *77*(4), 4295-4307. https://doi.org/10.1007/s11042-017-4766-y

[21] Liu, E., Liang, J., Pang, L., Xie, M., & Tian, J. (2010). Minutiae and modified biocode fusion for fingerprint-based key generation. *Journal of Network and Computer Applications*, *33*(3), 221-235. https://doi.org/10.1016/j.jnca.2009.12.002

[22] Li, X. L., Hu, Y. X., Yang, X., Yu, X. D., & Li, Q. L. (2014). A novel zinc-finger HIT protein with an additional PAPA-1-like region from Suaeda liaotungensis K. enhanced transgenic Arabidopsis drought and salt stresses tolerance. *Molecular Biotechnology*, *56*(12), 1089-1099. https://doi.org/10.1007/s12033-014-9789-2

Contact information:

Bing ZHENG, Master, Professor
School of Information Engineering,
Hainan Vocational University of Science and Technology,
Haikou, Hainan, China
E-mail: zhbahn@vip.qq.com

Zhenyu QIU, Master, Lecturer
(Corresponding author)
Applied Mathematics Research Department,
Nanchang Institute of Technology,
Nanchang, Jiangxi, China
E-mail: zb@hvust.edu.cn

Jing YANG, PhD, Associate Professor
School of Information Engineering,
Hainan Vocational University of Science and Technology,
Haikou, Hainan, China
Email: yangjing@hvust.edu.cn