Fingerprint Template Protection Using Multiple Spiral Curves

Munaga V.N.K. Prasad, Jaipal Reddy Anugu and C.R. Rao

Abstract In this paper we proposed a method for generating the cancelable fingerprint template using spiral curves by constructing contiguous right angled triangles using the invariant distances between reference minutia and every other minutiae in fingerprint image, then projecting onto a 4D space, features transformed using DFT. The proposed approach experimented by using the FVC database. The approach attains the primary needs diversity, revocability, security of biometric system. Performance is calculated using metrics GAR, FAR, and EER.

Keywords Fingerprint template generation · Contiguous right angled triangles · Projection · Transformation · Security

1 Introduction

Biometrics gained its popularity in secure authentication in comparison with traditional based methods of remembering tokens and passwords [1]. Biometrics traits are inextricably bound to individual's identity [2] and need not to remember. However, biometrics will be same forever, once compromised can not be reissued or canceled [1], thus violating user privacy. If biometrics lost everything lost. Individuals face threat to their physical existence as they can not be kept away from theft. This has raised problems and challenges in security and regarding protection of one's identity. Hence, there should be a biometric technique that ensures security and privacy. Any

M.V.N.K. Prasad (✉) · J.R. Anugu
Institute for Development and Research in Banking Technology, Hyderabad, India
e-mail: mvnkprasad@idrbt.ac.in

J.R. Anugu
e-mail: jaipalreddy51@gmail.com

J.R. Anugu · C.R. Rao
School of Computer and Information Sciences, University of Hyderabad, Hyderabad, India
e-mail: crrcs@uohyd.ernet.in

A. Nagar et al. (eds.), *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, Smart Innovation, Systems and Technologies 43, DOI 10.1007/978-81-322-2538-6_61

cancelable biometric method must meet the following characteristics [1] (i) Diversity, (ii) Revocability, (iii) Non-invertibility and (iv) Performance.

There are four categories of attacks [3] at sensor module, interface module, software module and database module. Irrevocability of template makes it more dangerous and violates user's privacy. Therefore, need of biometric technologies to provide increased security and privacy protection. The template protection schemes are broadly categorized into cancelable biometrics and biometric cryptosystem [3]. Cancelable biometrics is about to transform the features into irreversible template. The two approaches, namely biometric salting (blending user specific information like password or token with biometric data to generate a new template) and non-invertible transforms (transform original biometric data into irreversible template) are under cancelable biometrics. On other side, Biometric cryptosystem serves by securing cryptographic key with help of biometric data (key binding) or generating cryptographic key (key generation) [3] from biometric data.

The rest of paper is organized as follows: In Sect. 2, discussion regarding the related work done on cancelable biometrics. Section 3 explains about the proposed model. Section 4 explains the experimental setup and analysis of the model in terms of the performance characteristics of cancelable biometrics. Conclusions are discussed in Sect. 5.

2 Literature Review

Reconstruction of original fingerprint image from minutiae set was proved [4]. Later a many methods have come for reconstruction of fingerprint image from minutiae [5–7]. Because of feasibility to inversion, it is not secure to keep the original fingerprint features as biometric template. As an alternative layers of protection could be applied to original fingerprint to convert into new form. But, performance is generally degraded when transformations applied [8]. Preserving the performance while applying transformations being a challenging task.

In literature, there exists direct minutiae transformation and indirect minutiae transformation. In first case the original location and orientation are taken directly for further use; invariant features taken in later case. For feature transformation, [8] proposed first method to generate biometric template using non-invertible transform functions, namely Cartesian, polar and surface-folding transformation. Though the three transformations claimed to be non-invertible, later an approach [9] reveals the invertibility of surface folding transformation if parameters and transformed template are known.

In method [10], a 3D array taken, for each reference minutia other minutiae are translated and rotated. Each cell is marked as '1' if it contains more than one minutiae falling in each cell, otherwise '0'. For same key scenario the performance degraded significantly. A method alignment free fingerprint template [11], the calculated invariant feature set is given as input to user specific transformation function to derive parameters, which can be used to generate cancelable template. Generation of revocable fingerprint template using minutiae triplet [12]. Similarly, revocable fingerprint template generation [13] by taking four invariant features from minutia pair and then using histogram binning [14].

Pair polar coordinate based scheme [15] explores the relative relationship of minutiae in a rotation and shift-free pair-polar framework. Non-inversion is attained through many-to-one mapping relation. The method based on densely infinite-to-one mapping (DITOM) technique [16] elaborates the three features, then quantized, hashed, and binarized using histogram binning. Method based on curtailed circular convolution [17] where generation of random sequence using user specific key, L-point Discrete Fourier Transform (DFT)s of bit-string and random sequence independently, then taking inverse DFTs on the product of DFTs generated. Considered the points as template after removing first p-1 points.

The work of multiline code (MLC) [18] enhanced [19] by taking mean distance of minutiae falling in each semicircle region along the lines. Performed quantization to get bit-string, then permutation of resulted bit-string using user key. Multiline neighboring relation [20] by constructing rectangles with different orientations, followed by determining invariant distances and relative orientations, then projecting on to 2D plane, then transformation using DFT to get template.

3 Proposed Method

The steps involved in proposed method are as follows:

1. Construction of spiral curves.
2. Projection on to 4D space and bit-sting generation.
3. Feature transformation.
4. Matching.

3.1 Construction of Spiral Curve

Fingerprint feature extraction from impression. The minutiae set $N = [x_i, y_i, \theta_i]_1^k$, where k represents minutiae count in fingerprint image. Choose a reference minutia from the set, N.

1. Find out the rotation and translation invariant distance between reference minutia, (x_r, y_r, θ_r) and the every other minutiae (x_i, y_i, θ_i) in image.

$$\begin{bmatrix} x_i^T \\ y_i^T \end{bmatrix} = \begin{bmatrix} \cos\theta_r & -\sin\theta_r \\ \sin\theta_r & \cos\theta_r \end{bmatrix} \begin{bmatrix} (x_i - x_r) \\ -(y_i - y_r) \end{bmatrix} \quad (1)$$

Based on the calculated values x_i^T and y_i^T, distance is evaluated $d_{ri} = \sqrt{x_i^{T^2} + y_i^{T^2}}$.

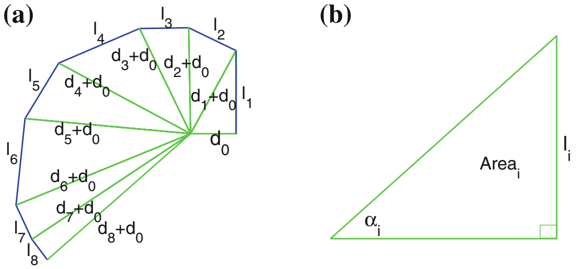

Fig. 1 **a** Construction of spiral curve for reference minutia. **b** Metrics in triangle

2. Sort the distances in ascending order, take n number of least distances to draw contiguous right angled triangles taking distances as hypotenuses of triangles [21]. For first triangle, the base distance is taken as specific value d_0 and the same is added to every distance as shown in Fig. 1a.
3. The other side of triangle, l_i as shown in Fig. 1a is calculated using Pythagoras theorem. We keep the distance l_i, angle at vertex as center α_i, area A_i of each triangle as shown in Fig. 1b and the actual orientation of corresponding minutiae θ_i as feature set for further use.
4. For each reference minutia, (x_r, y_r, θ_r) we represent the feature set as $L_r = [[l_{r1}, \theta_1, \alpha_{r1}, A_{r1}], [l_{r2}, \theta_2, \alpha_{r2}, A_{r2}], \ldots [l_{rn}, \theta_n, \alpha_{rn}, A_{rn}]]$, where $l_{ij}, \alpha_{ij}, A_{ij}$ indicates the metrics taken for each triangle, θ_j indicates the orientation of corresponding minutia from which we have taken invariant distance to reference minutia, n is the number of minutiae taken after sorting the distances.
5. Repeat the steps 1–4 for each other minutiae in minutia set, N of a fingerprint. Thus fingerprint template contains $L = [L_1, L_2, L_3, \ldots, L_k]$ where k refers minutiae count in fingerprint image.

Here, in the feature set we are storing metrics of each triangle and orientations of minutiae. From the feature set we can not find the position and orientation of minutia in the fingerprint image.

3.2 Projection on to 4D Space and Bit-Sting Generation

We generate bit-string by using space based quantization. Each L_r is a vector of order 4, $L_r = (l_{ij}, \theta_j, \alpha_{ij}, A_{ij})$, can be plotted on a 4D-space by taking distance, orientation, angle and area along 4 axes in space with ranges in [0 λ], [0 360], [0 90] and [0 Δ] respectively, where λ is maximum distance and Δ is maximum area. The cells of 4D-space are partitioned into sizes cx, cy, cz and cw along axes [10]. The number of cells in the plane are $A \times B \times C \times D$ where $A = \left\lfloor \frac{maximum\,distance}{cx} \right\rfloor$, $B = \left\lfloor \frac{360}{cy} \right\rfloor$, $C = \left\lfloor \frac{90}{cz} \right\rfloor$ and $D = \left\lfloor \frac{maximum\,area}{cw} \right\rfloor$. Here $\lfloor . \rfloor$ represents the floor function. The template L is mapped to 4D space. Then we will know which cell contains which points on the plane using the Eq. 2.

$$\begin{bmatrix} x_i \\ y_i \\ z_i \\ w_i \end{bmatrix} = \begin{bmatrix} \lfloor l_{ij}/cx \rfloor \\ \lfloor \theta_j/cy \rfloor \\ \lfloor \alpha_{ij}/cz \rfloor \\ \lfloor A_{ij}/cw \rfloor \end{bmatrix} \tag{2}$$

where x_i, y_i, z_i and w_i indicate the x, y, z and w indices on 4D space, cx, cy, cz and cw represents the dimensions of each cell. By visiting each and every cell of 4D space we will get a binary string by taking ‘1’ for one or more point falling onto a cell, otherwise ‘0’. So the length of bit-string will be I = $A \times B \times C \times D$.

3.3 Feature Transformation

The generated bit-string need to be transformed into non-invertible template for protection. Apply Discrete Fourier Transform on bit-string (H_w) to transform into a complex vector. Performing I-point DFT on H_w, we get frequency domain complex vector, F_i into $I \times 1$ vector. $F = [F_0, F_1, F_2, \ldots, F_{I-1}]$. Multiply the user specific random matrix R with complex vector F to transform into non-invertible template T [16]. $[T]_{p\times 1} = [R]_{p\times q}[F]_{q\times 1}$. Here q = I, the size of bit-string and $p < q$. Thus T is a transformed vector of order $p \times 1$. While at verification we use the same user key to generate the random matrix and then to generate transformed template.

3.4 Matching

Local matching In Local matching, we compare template locally by matching each spiral curve data in enrolled template with every spiral curve data in query template. Fingerprint transformed templates at the time of enrollment and query are represented as $E = [E_1, E_2, E_3, \ldots, E_m]$ and $Q = [Q_1, Q_2, Q_3, \ldots, Q_n]$. Then the distance between both of E_i and Q_j is calculated using Eq. 3

$$d(E_i, Q_j) = \frac{\|E_i - Q_j\|_2}{\|E_i\|_2 + \|Q_j\|_2} \tag{3}$$

where $\|.\|_2$ indicates 2-norm or euclidean norm. Then the matching score can be found using $S(E_i, Q_j) = 1 - d(E_i, Q_j)$. The matching score will come in range of [0 1]. Matching is done according to [19, 20]. To prevent double matching we re-evaluate similarity matrix. $S(E_i, Q_j) = S(E_i, Q_j)$ if $S(E_i, Q_j)$ is maximum for $j \in [1, m]$ and $i \in [1, n]$, otherwise 0.

Global matching In global matching we take the maximum similarity score of the template comparison using Eq. 4. Here Ψ indicates the count of non-zero values in $S(E_i, Q_j)$, m and n are minutiae counts in respective enrolled and query templates. If score is 1, refers exact match and 0 refers mismatch.

$$MS = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} S(E_i, Q_j)}{\Psi} \tag{4}$$

4 Experimental Results and Analysis

For experimental testing database collected at Fingerprint Verification Competition: FVC2002. Each DB1, DB2, DB3 contains 100 users with 8 samples each. We took 2 impressions per each user. Neurotechnology Verifinger SDK used to extract features. False Rejection Rate (FRR), Genuine Acceptance Rate (1-FRR), False Acceptance Rate (FAR), Equal Error Rate (EER) are measures of performance [1]. FRR is the ratio of total false rejections to total identification attempts or the probability of rejecting a similar image as impostor. FAR is the ratio of total false acceptances to total identification attempts or the probability of accepting dissimilar image as genuine. EER is the value when FRR and FAR are equal. Genuine Acceptance Rate is accepting similar image as genuine.

In the method we have taken minutiae points as center for drawing spiral curves instead of singular points [21] which may not be available in all images. Considered only 4 smallest distances instead of all distances for each reference minutia to reduce complexity. In quantization after fine tuning cx, cy, cz and cw are fixed. In different key scenario we got EER value 0 %. For same key scenario EER values are shown in Table 1. Figure 2 refers the error rate for FVC2002. Receiver Operating Characteristic (ROC) curve for FVC2002 DB1, DB2 and DB3 as in Fig. 3, shows that low recognition rate for DB3 relative to DB1 and DB2 because of low quality images. The proposed model ensures the revocability and diversity by changing user key to generate multiple templates which can not be matched. Using different keys 100 transformed templates are generated from a same image on FVC2002 DB2 and matched with enrolled image to find pseudo-imposter

Table 1 Equal error rate for same key scenario

Methods	FVC2002		
	DB1	DB2	DB3
Ahmed et al. [15]	9	6	27
Yang et al. [22]	–	13	–
Jin et al. [13]	5.19	5.65	–
Proposed method	7.85	5.29	17.55

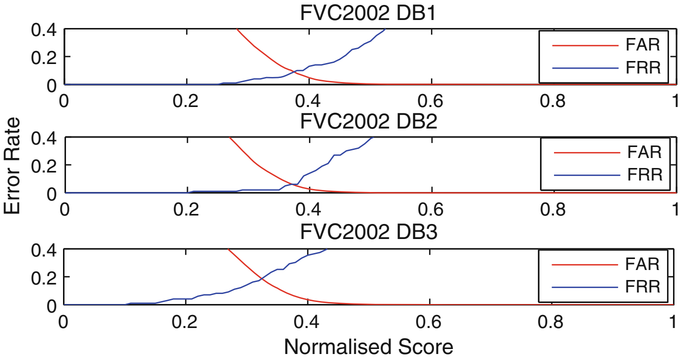

Fig. 2 Equal error rate for FVC2002 same key

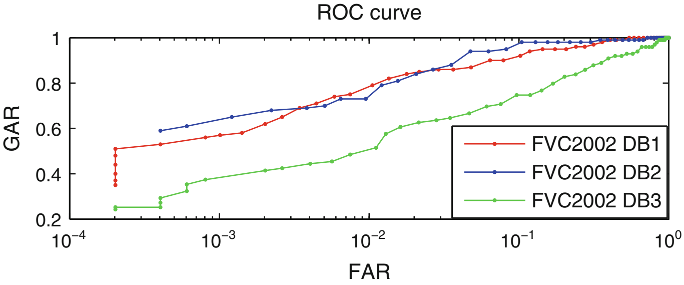

Fig. 3 ROC curve for same key for FVC2002

distribution. As shown in Fig. 4 pseudo-imposter distribution is clearly separated from genuine distribution. In security perspective it is inconceivable to regress original image from a stolen template. Even if adversary knows the spiral curves of each reference minutia, the position of reference minutia and orientation can not be found to try the possibilities to put neighboring minutiae around it.

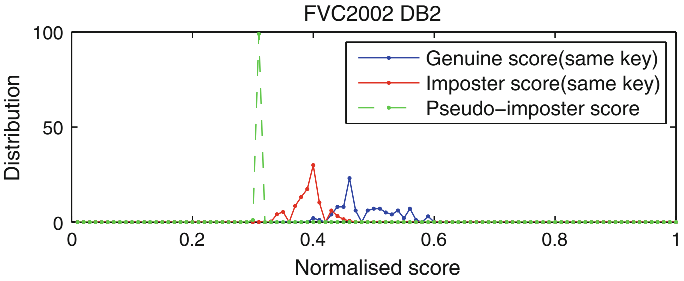

Fig. 4 Genuine, imposter and pseudo-imposter distributions for FVC2002 DB2

5 Conclusion

We proposed a technique to protect fingerprint template. We represented the spiral curves model [21] in different perspective by considering minutiae points as center to shell. We then taken information from triangles to project on to the space based quantization to get bit-string, and then generated cancelable templates. This method meets requirements security, revocability and diversity of biometric system. EER for different key scenario is 0 %. EER for FVC2002 DB2 is 5.29 %.

References

1. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition, 2nd edn. Springer, Heidelberg (2009)
2. Jain, A.K., Ross, A.A., Nandakumar, K.: Introduction to Biometrics. Springer (2011)
3. Jain, A.K., Nandakumar, K.: Biometric template security, EURASIP. J. Adv. Signal Process. 1–17 (2008). Article ID: 579416
4. Hill, C.: Risk of masquerade arising from the storage of biometrics (Masters thesis), Australian National University (2001)
5. Ross, A.K., Shah, J., Jain, A.K.: From template to image: reconstructing fingerprint from minutiae points. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 544–560 (2007)
6. Cappelli, R., Lumini, A., Maio, D., Maltoni, D.: Fingerprint image construction from standard templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**(9), 1489–1503 (2007)
7. Feng, J., Jain, A.K.: Fingerprint reconstruction: from minutiae to phase. IEEE Trans. Pattern Anal. Mach. Intell. **33**(2), 209–223 (2011)
8. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating cancelable fingerprint templates. IEEE Tans. Pattern Anal. Match. Intell. **29**(4), 561–572 (2007)
9. Fenq, Q., Su, F., Cai, A., Zhao, F.F.: Cracking cancelable fingerprint template of Ratha. In: International Symposium on Computer Science and Computational Technology (ISCSCT08), vol. 2, pp. 572–575 (2008)
10. Lee, C., Kim, J.: Cancelable fingerprint templates using minutiae based bit strings. J. Netw. Comput. Appl. **33**, 236–246 (2010)
11. Lee, C., Choi, J.Y., Toh, K.A., Lee, S., Kim, J.: Alignment-free cancelable fingerprint template based on local minutia information. IEEE Trans. Syst. Man. Cybern.-Part B: Cybern. **37**(4), 980–992 (2007)
12. Farooq, F., Bolle, R.M., Jea, T.Y., Ratha, N.K.: Anonymous and revocable fingerprint recognition. In: Proceeding of the International Conference on Computer Vision and Pattern Recognition, pp. 1–7 (2007)
13. Jin, Z., Teoh, A., Ong, T.S., Tee, C.: Fingerprint template protection using minutia-based bit-string for security and privacy preserving. Expert Syst. Appl. **39**, 6157–6167 (2012)
14. Jin, Z., Teoh, A., Ong, T.S., Tee, C.: A revocable fingerprint template for security and privacy preserving. KSII Trans. Internet Inf. Syst. **4**(6), 1327–1341 (2010)
15. Ahmed, T., Hu, J., Wang, S.: Pair-polar coordinate based cancelable fingerprint templates. Pattern Recogn. Lett. **44**, 2555–2564 (2011)
16. Wang, S., Hue, J.: Alignment free cancelable fingerprint template design: a densely infinite to one mapping (DITOM) approach. Pattern Recogn. **45**, 4129–4137 (2012)
17. Wang, S., Hu, J.: Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recogn. **47**, 1321–1329 (2014)

18. Wong, W.J., Wong, M.L.D., Kho, Y.H.: Multiline code: a low complexity revocable fingerprint template for cancelable biometrics. J. Cent. South Univ. **20**, 1292–1297 (2013)
19. Wong, W.J., Teoh, A.B.J., Wong, M.L.D., Kho, Y.H.: Enhanced multiline code for minutiae based fingerprint template protection. Pattern Recogn. Lett. **34**, 1221–1229 (2013)
20. Prasad, M.V.N.K., Kumar, C.S.: Fingerprint template protection using multiline neighboring relation. Expert Syst. Appl. **41**, 6114–6122 (2014)
21. Moujahdi, C., Bebis, G., Ghouzali, S., Rziza, M.: Fingerprint shell secure representation of fingerprint template. Pattern Recogn. Lett. **45**, 189–196 (2014)
22. Yang, H., Jiang, X., Kot, A.C.: Generating secure cancelable fingerprint templates using local and global features. In: 2nd IEEE ICCSIT, pp. 645–649 (2009)