Coprime Mapping Transformation for Protected and Revocable Fingerprint Template Generation

Rudresh Dwivedi(✉) and Somnath Dey

Discipline of Computer Science and Engineering, Indian Institute of Technology Indore, Indore 453446, India
{phd1301201006,somnathd}@iiti.ac.in

Abstract. Compromise of biometric data may cause permanent loss of identity since the biometric information is intrinsically linked with the user. To revoke the stolen biometric template, the concept of cancelable biometrics has been introduced. The idea behind cancelable biometric is to transform the original biometric template into a new template and perform matching in the transformed domain. In this paper, a coprime transformation scheme has been proposed to generate the cancelable fingerprint template. The method divides the fingerprint region into a number of sectors with respect to each minutiae point and identifies the nearest-neighbor minutiae in each sector. Then, ridge-based features for all minutiae points are computed and mapped onto co-prime positions of a random matrix to generate the cancelable template. The proposed approach achieves an EER of 1.82, 1.39, 4.02 and 5.77 on DB1, DB2, DB3 and DB4 datasets of the FVC2002 database, respectively. Experimental results indicate that the method outperforms in comparison to the current state-of-the-art. Moreover, the proposed method fulfills the necessary requirements of diversity, revocability, and non-invertibility with a minor performance degradation caused by the transformation.

Keywords: Biometric · Fingerprint verification · Template protection

1 Introduction

1.1 Background

Compromising the stored biometric template causes permanent losing his/her identity due to irreplaceable and irrevocable characteristics of original biometric data. There are several privacy issues associated with the sharing of biometric information across many applications [1]. Therefore, it is necessary to provide biometric template protection. The concept of cancelable biometric has been introduced for template protection which state that a transformed template is required to be stored instead of the original biometric template. The transformation relies on an irreversible function such that it is difficult to discover the original template even if the attacker discovers the transformation function and the transformed template. In the case of compromise, a new template can be

A. Ghosh et al. (Eds.): MIKE 2017, LNAI 10682, pp. 111–122, 2017.
https://doi.org/10.1007/978-3-319-71928-3_12

derived by altering the parameter values of the transformation function. Further, it should not exhibit significant performance degradation in comparison to the true biometric system.

1.2 Existing Approaches

Recently, various approaches for cancelable template design have been proposed in the literature. Ratha et al. [1] introduced cartesian, polar, and functional transformation for fingerprint template security. Das et al. [2] introduced a graph structure based on the nearest-neighbor distance from core point to all other minutiae points. However, the methods proposed by Ratha [1] and Das et al. [2] require core point to align two fingerprints before transformation. However, the detection of the core point is not always possible.

Lee et al. [3] proposed a method to map aligned minutiae points into a 3-D array based on the minutiae orientation and difference between minutiae coordinates. The array is visited in sequence to derive a bit-string which is permuted based on a user-specific PIN and the type of minutiae. In the alignment-free method proposed by Wang et al. [4], pair-minutiae vectors are quantized, indexed and converted to bit-string. Then, a user specific PIN is applied to the complex vector derived by taking discrete Fourier transform onto bit-string. Moujahdi et al. [5] proposed fingerprint shell which utilizes the distance between the singular point and all other minutiae points. The distances with an addition of user-specific key are sorted in ascending order to derive spiral curve. In another work, Wang et al. [6] presented a way to protect the bit-string derived using the method proposed in [4]. The bit-string is utilized as an input to FIR filter with a user-specific key. The performance of the methods proposed in [3–6] degrades if user-specific token is compromised. Further, Wang et al. [7] proposed a method which utilizes the partial Hadamard transform to the derived bit string.

Cappelli et al. [8] proposed a novel minutiae representation MCC (Minutiae cylinder Code) which constructs a 3-D cylindrical structure around each minutiae neighborhood. Later, Ferrara et al. [9] proposed protected-MCC (P-MCC) which applies binary-KL projection onto MCC templates to overcome security concerns against non-invertibility in MCC [8]. However, further investigations unveil the irrevocability issue of P-MCC. To achieve revocability, Ferrara et al. [10] proposed two-factor protected Minutiae Cylinder-Code (2P-MCC) which performs partial permutation using a secret key over the cylinders in P-MCC.

1.3 Contributions

To alleviate the issues of the existing methods described above, we propose a novel cancelable fingerprint template generation method based on coprime mapping transformation. Our contributions in this work are highlighted in the following:

(1) Ridge features are evaluated under ridge coordinate system to deal with rotation, scale and translation distortions in the input fingerprint image.

(2) The proposed work does not rely on pre-alignment of the core or singular points as it is hard to detect the singularities in poor quality fingerprint images.
(3) The nearest-neighbor transformation is applied around each minutia to derive a fixed length descriptor instead of fixed-radius transformation. This overcomes the limitation of performance degradation caused due to the border minutiae points.
(4) We have tested our approach with respect to the desirable criteria for cancelable transformation i.e. revocability, irreversibility, and diversity.
(5) The performance of the proposed method is evaluated on all datasets of FVC2002. The experimental results show that our approach performs better than the existing approaches.

The organization of this paper is as follows. Section 2 describes the proposed scheme for cancelable template generation. Experimental results are demonstrated in Sect. 3. Section 4 presents the security analysis. Concluding remarks and course of future work are described in Sect. 4.

2 Proposed Scheme

The overall design for the proposed method is illustrated by the block diagram shown in Fig. 1. The proposed method consists of three main tasks including pre-processing and minutiae extraction, feature extraction, and cancelable template generation.

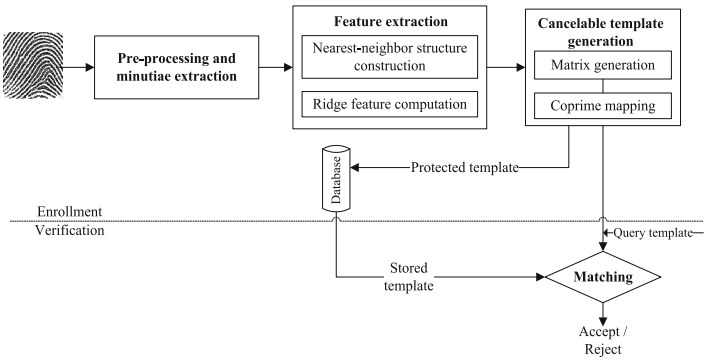


Fig. 1. Block diagram of the proposed method

2.1 Pre-processing and Minutiae Extraction

In this work, pre-processing and minutiae point extraction is performed by the approach described in [11]. The minutia points are represented as:

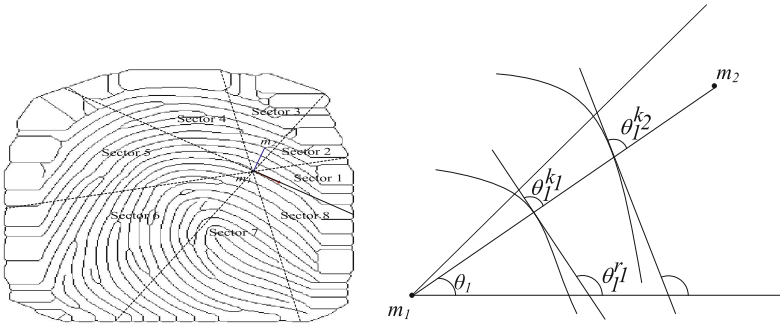
$$V_{up} = \{m_i\}_{i=1}^{n}$$
$$m_i = (x_i, y_i, \theta_i) \tag{1}$$

where, V_{up} is a set of unprotected minutiae points derived from a fingerprint image, m_i is the i^{th} minutiae point and n is the total number of minutiae points in V_{up}. The minutiae point m_i is represented by the coordinate (x_i, y_i) and the minutiae orientation θ_i. The preprocessing task also outputs a thinned fingerprint image which is utilized for feature extraction.

2.2 Feature Extraction

There is a necessity to compute transformation invariant features from a fingerprint image since performance could degrade by rotation, translation and scaling transformation caused at the time of acquisition. In this work, we compute ridge features to deal with rotation and scale deformations present in the input fingerprint image. Feature extraction involves two steps: nearest-neighbor structure construction and ridge feature computation.

Nearest-Neighbor Structure Construction: After the preprocessing task, we obtain the thinned output image and minutiae information from the input fingerprint. One of the minutiae from the minutiae set V_{up} is considered as a reference minutiae. Next, we construct the nearest-neighbor structure around the reference minutiae point utilizing ridge coordinate system as shown in Fig. 2(a). The ridge coordinate system allocates the reference axis coinciding with the orientation of the selected minutiae. Further, the fingerprint region is divided into 's' sectors of equal angular displacement utilizing ridge coordinate system as displayed in Fig. 2(a).



(a) Nearest-neighbor structure for $s = 8$ (b) Ridge-based feature computation

Fig. 2. Feature extraction

Ridge Feature Computation: First, each minutia is considered as a reference. Next, ridge count and average ridge orientation between reference minutiae and nearest minutiae in each sector are calculated. Ridge count is evaluated by counting the ridges between reference minutiae and nearest neighbor minutia. For example, ridge count between two minutiae points (say m_1 and m_2) is 2 as shown in Fig. 2(b). To compute ridge orientation, the angle subtended by the tangent line and the straight line connecting two minutiae points is measured for each ridge crossing. For example, the orientation of the first ridge in the first sector as shown in Fig. 2(b), θ_1^{k1} can be evaluated as:

$$\text{for sector 1: } \theta_1^{k1} = \theta_1^{r1} - \theta_1$$

where θ_1 is the slope of the line connecting reference minutiae and nearest neighbor minutia in the first sector. θ_1^{r1}, is the angle subtended by the tangent line from the intersection point of first ridge and reference axis. Similarly, we can find out the orientation of second ridge, θ_1^{k2} and evaluate the mean ridge orientation for example shown in Fig. 2(b). The mean ridge orientation for each sector can be formulated as defined in Eq. (2).

$$\text{for } i^{th}, \text{sector: } r_{or_i} = \frac{\left(\theta_i^{r1} - \theta_i\right) + \left(\theta_i^{r2} - \theta_i\right) + \ldots\ldots + \left(\theta_i^{rNr_i} - \theta_i\right)}{Nr_i} \tag{2}$$

where Nr_i is the total number of ridges between the reference and nearest minutiae in the i^{th} sector. We store the ridge features into a 2-D matrix (F). For example, if a fingerprint image contains n minutiae points then, the feature matrix F will contain $n \times 2s$ entries including s ridge count and s average ridge orientation considering s sectors in a fingerprint image. We assign zero to the ridge features corresponding to a sector if no minutia point is located in that sector. At the time of matching, we do not consider the sectors with no minutiae point.

2.3 Cancelable Template Generation

The generation of cancelable fingerprint template involves two tasks: matrix generation and co-prime mapping.

Matrix Generation: We map the feature matrix into a high-dimensional matrix to derive the protected template. For this purpose, a random matrix $CanTemp$ of size $T \times T$ is generated with a seed (ρ). The value of T is equal to $n \times 2s$ where n and s are the total number of minutiae points in the input fingerprint image and the number of sectors around a reference minutiae, respectively.

Co-prime Mapping: We map the feature matrix $F_{n \times 2s}$ into $CanTemp$ such that there will be no overlapping. To perform this, we use co-prime based mapping in our method which maps all elements of F at T places of $CanTemp$.

Rest of the entries of matrix are filled with is filled with some random data. The following four keys are utilized for mapping:

(1) k_1: initial row position (2) k_2: initial column position (3) k_3: number of row jump from initial position (4) k_4: number of column jump from initial position.

The start position is calculated based on the user-specific key. We start at position (k_1, k_2) in matrix $CanTemp$. The next position (NP) is computed based on the row and column jump to the initial position using the following relation described in Eqs. (3) and (4):

$$NP_i = \begin{cases} k_1 + k_3 & if\,(k_1 + k_3 \leqslant T) \\ k_1 + k_3 - T & if\,(k_1 + k_3 > T) \end{cases} \tag{3}$$

$$NP_j = \begin{cases} k_2 + k_4 & if\,(k_2 + k_4 \leqslant T) \\ k_2 + k_4 - T & if\,(k_2 + k_4 > T) \end{cases} \tag{4}$$

To avoid overlapping in the matrix, the co-prime mapping is adopted. In this technique, we select the value of k_3 and k_4 such that both should be co-prime with T as defined in Eq. (5).

$$\begin{aligned} GCD\,(k_3, T) &= 1 \;\forall\; k_3 \epsilon [2, T] \\ GCD\,(k_4, T) &= 1 \;\forall\; k_4 \epsilon [2, T] \end{aligned} \tag{5}$$

For example, if the key values for start position are $k_1 = 2$ and $k_2 = 2$, respectively and the key values for row and column jump are $k_3 = 3$, $k_4 = 5$, then the co-prime based mapping is shown in Fig. 3.

	1	2	3	4	5	6	7	8
1	1	0	5	9	3	1	10	19
2	6	**2**	3	7	11	15	28	32
3	0	7	7	0	8	12	11	17
4	9	4	9	4	7	0	17	8
5	6	5	6	4	12	10	**45**	19
6	4	8	3	11	19	5	27	14
7	2	7	1	0	22	3	34	21
8	8	4	0	**6**	11	7	19	14

Fig. 3. Example of co-prime based mapping procedure

2.4 Matching

Fingerprint matching refers to the process of comparing an enrolled fingerprint template (say CT) and a query fingerprint template (say QT) to return a matching score. In our method, matching is performed in two steps: Local matching and global matching.

Local Matching: In local matching, ridge feature set corresponding to a minutiae point from QT is compared with ridge feature set for a minutiae point of CT to return local match score. Mapped ridge feature set in the QT and CT are accessed using user-specific keys k_1, k_2, k_3 and k_4. We compute the Euclidean distance between the mapped non-zero entries of the query and enrolled template. Next, we compute the mean of the minimum distances corresponding to each non-zero entries of the two ridge features sets of CT and QT as described in Eq. (6).

$$e\_dist = \sqrt{(QT_N[i][1] - CT_M[j][1])^2 + (QT_N[i][2] - CT_M[j][2])^2} \tag{6}$$

Global Matching: In global matching, we compute the number of matched minutiae points between QT and CT utilizing the local match scores by comparing each ridge-feature set from QT with each ridge-feature set from CT. Next, overall matching score is evaluated by the number of matched minutiae points divided by the number of minutiae points in QT as described in Eq. (7).

$$overall\_match\_score = \frac{match\_minutiae\_count}{N} \tag{7}$$

3 Experimental Results and Analysis

In our experiment, we use four datasets DB1, DB2, DB3 and DB4 of FVC2002 database [12] since the most of the existing approaches utilized these datasets. Each datasets DB1, DB2, DB3 and DB4 of FVC2002 contains a total of 800 images of 100 subjects with eight samples each. The performance of the method is evaluated with four parameters: False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER) which is defined as the error rate when the FRR and FAR holds equality, and GAR is computed as 1-FRR.

3.1 Validation of Parameter: Number of Sectors (s)

After the preprocessing steps, the proposed method divides the input fingerprint image into the s number of sectors with equal angular width. To validate the parameter s, we have performed a number of experiments considering distinct angular widths. We have computed the EER with angular width of 15°, 30°,... and 90° corresponding to $s = 24, 12,...$ and 4, respectively. The performance for the different number of sectors is reported in Table 1. It has been observed that the method performs the best for $s = 8$ on each of the datasets of FVC2002. It has also been observed that for high values of s, EER increases as there are more number of sectors without minutiae points. Therefore, we have considered $s = 8$ for all other experiments.

Table 1. EER obtained for databases FVC 2002 DB1, DB2, DB3 and DB4 in same key scenario

Number of sectors (s)	EER (in %)			
	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2002 DB4
4	3.93	3.79	5.86	6.83
8	**1.82**	**1.39**	**4.02**	**5.77**
16	5.04	4.93	8.83	12.7
32	9.63	5.19	11.24	19.3

3.2 Performance

We have followed FVC protocol to evaluate our method which compares each subject against the first sample of the remaining subjects to calculate impostor scores and each sample is compared against the remaining samples of the same subject to calculate the genuine score. Therefore, 4950 and 2800 impostor and genuine comparisons are required respectively if all samples are enrolled for each set of the FVC2002 database. Further, we have conducted the experiments under two scenarios to evaluate the performance of our method: Same key scenario and different key scenario.

Same Key Scenario: In this scenario, we assume that a user's key is stolen. In this case, an imposter utilizes the key as a genuine user to gain access into the system. To rectify this attack, we apply same keys (i.e. k_1, k_2, k_3 and k_4) to enroll all users. The proposed method is applied onto DB1, DB2, DB3 and DB4 dataset of database FVC2002. Figure 4 represents the ROC curves for each dataset of FVC2002 for the optimal value of parameter s (i.e. $s = 8$).

For FVC2002 database, we achieve an EER of 1.82, 1.39, 4.02, and 5.77 for DB1, DB2, DB3, and DB4, respectively using FVC protocol. Out of all FVC2002 datasets, the method performs better on DB1 and DB2 as these datasets contain more number of good quality images as compared to datasets DB3 and DB4. Further, the dataset DB3 and DB4 contain less number of minutiae points per image due to poor quality images as compared to dataset DB1 and DB2. As a result, we achieve high EER for DB3 and DB4 datasets.

Different Key Scenario: To test our method in different key scenario, we use different keys (i.e. k_1, k_2, k_3 and k_4) to enroll different users. We obtain an EER of 0 for DB1, DB2 and DB4 datasets and an EER of 0.09 for the dataset DB3 of FVC2002. Therefore, it is evident that our approach performs better in the different key scenario.

3.3 Baseline Comparison

For baseline comparison, we perform two set of experiments. In the first experiment, we compute the EER using the original fingerprint template comprising

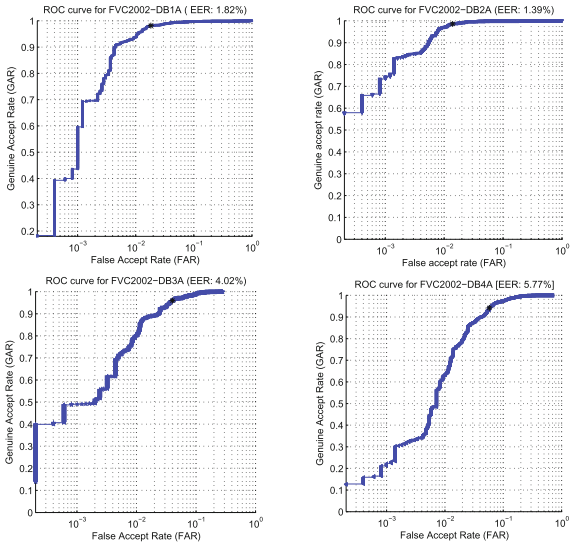


Fig. 4. ROC curves for FVC 2002 DB1, DB2, DB3 and DB4 under same key scenario

ridge features. In the second experiment, we apply coprime mapping transformation utilizing the keys (k_1, k_2, k_3 and k_4) and evaluate the performance. Table 2 shows that the performance is degraded by 0.19%, 0.41%, 0.05%, and 0.39% for DB1, DB2, DB3, and DB4 dataset of FVC2002 database, respectively. From the reported results, it is evident that the performance degradation caused by the transformation is very low.

Table 2. Baseline comparison for FVC2002 database

FVC2002	EER (in %)		Performance degradation
	Without cancelable transformation	With cancelable transformation	
DB1	1.47	1.82	0.19
DB2	0.89	1.39	0.41
DB3	3.81	4.02	0.05
DB4	3.49	5.77	0.39

3.4 Comparison with Existing Approaches

The proposed method is compared with methods [2–7, 9, 10] described in Sect. 1. Table 3 shows the comparison in terms of EER. From Table 3, it has been observed that the proposed method performs better as compared to the

approaches proposed in [2,3,5,10]. However, the performance of our method is slightly lower than the approach in [9,13] yet comparable to the existing template protection approaches. Therefore, from the reported results it is evident that our approach outperforms over the existing methods.

Table 3. EER obtained for databases FVC 2002 DB1, DB2, DB3 and DB4 in same key scenario

Methods	EER (in %)			
	FVC2002 DB1	FVC2002 DB2	FVC2002 DB3	FVC2002 DB4
Das et al. [2]	2.27	3.79	-	-
Moujahdhi et al. [5]	4.28	1.45	-	-
Wang et al. [4]	3.5	5	7.5	-
Lee et al. [3]	10.3	9.5	6.8	-
Wang et al. [6]	3	2	7	-
Wang et al. [7]	1	2	5.2	-
Ferrara et al. [9]	1.88	0.99	5.24	4.84
Ferrara et al. [10]	3.3	1.8	7.8	6.6
Proposed method	**1.82**	**1.39**	**4.02**	**5.77**

'–' indicates that the author(s) have not reported the results or results are reported for the partial dataset, in their work.

4 Security Analysis

A cancelable biometrics system needs to satisfy the criteria of irreversibility, revocability, and diversity as described in Sect. 1. In the following subsections, we will analyze our method with respect to these criteria.

4.1 Irreversibility Analysis

To analyze the irreversibility, we assume that an adversary is able to reveal the stored protected template $CanTemp$. In this case, the attacker cannot be able to reveal original template (F) as he does not have any information about the four keys utilized for mapping. For example, if the fingerprint image contains 50 minutiae points and it is divided into 8 sectors then the original template (F) and protected template $CanTemp$ would contain 800 cells and 640000 cells, respectively. It is very hard to compute initial positions (k_1, k_2) and next positions (k_3, k_4) to retrieve the entries of original template as there are $640000 \times 640000 = 409$ billion brute force attempts are required.

Further, if the attacker reveals the keys (k_1, k_2, k_3 and k_4) utilized for mapping. In this case, the attacker cannot be able to derive original template since keys k_1, k_2, k_3 and k_4 comprise of random coprime entries. From random coprime entries, it is impossible to retrieve any information about the original template.

4.2 Revocability Analysis

The revocability states that a new template must be issued if a stored protected template is compromised. To test the revocability of the method, we derived 100 different transformed templates by varying the parameter values from the same fingerprint. Next, genuine, imposter and Pseudo-imposter distribution are calculated for the FVC2002-DB1 dataset. From the experiment, we achieve 0% average FAR. The mean and standard deviation $(\mu; \sigma)$ of genuine, imposter and pseudo-imposter are 0.3931; 0.019, 0.9231; 0.0326, and 0.891; 0.0376, respectively. From the computed distribution, we observe that there is a strong overlap between the pseudo-impostor and impostor distributions as shown in Fig. 5. This implies that the templates derived with different keys from the same subject are different enough to prevent the cross-matching attack. Therefore, it can be stated that the transformed template differs from the compromised template although derived from the same fingerprint.

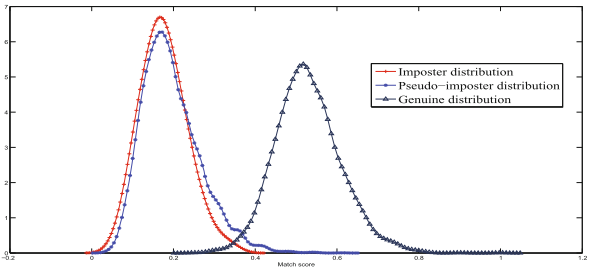


Fig. 5. Genuine, imposter and pseudo-imposter distribution for FVC2002 DB2

4.3 Diversity Analysis

It is essential that it should derive numerous templates without allowing cross-matching over various applications. Numerous different templates can be achieved by altering the key values (k_1, k_2, k_3, k_4) and seed value (ρ). Moreover, a change in the number of sectors (s) also suffices the generation of numerous templates.

5 Conclusion

In this paper, we have proposed a novel cancelable fingerprint template generation technique. The proposed technique does not depend on detection of singularities (core/delta). In this method, the input fingerprint image is divided into a number of sectors of equal angular partition. Invariant ridge features for the nearest neighbor minutiae in each sector are computed considering each minutia as a reference. Further, ridge features are mapped into a higher dimension

random matrix in coprime manner to derive the protected template. Experiments carried out over DB1, DB2, DB3 and DB4 datasets of FVC2002 database show a significant performance improvement as compared to the current state-of-the-art. Further, the security analysis ensures that our approach fulfills the necessary criteria for template protection schemes preserving the recognition accuracy. However, the computation of ridge feature for low-quality fingerprint and partial fingerprint images is a challenging task. This would be our future research direction.

Acknowledgment. The authors are thankful to SERB (ECR/2017/000027), Deptt. of science & Technology, Govt. of India for providing financial support to carry out this research work. Also, we would like to thank Kamal Meena and Rajesh Verma for coordinating and working with us.

References

1. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**(4), 561–572 (2007)
2. Das, P., Karthik, K., Chandra Garai, B.: A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. Pattern Recogn. **45**(9), 3373–3388 (2012)
3. Lee, C., Kim, J.: Cancelable fingerprint templates using minutiae-based bit-strings. J. Netw. Comput. Appl. **33**(3), 236–246 (2010)
4. Wang, S., Hu, J.: Alignment-free cancelable fingerprint template design: a densely infinite-to-one mapping approach. Pattern Recogn. **45**(12), 4129–4137 (2012)
5. Moujahdi, C., Bebis, G., Ghouzali, S., Rziza, M.: Fingerprint shell: secure representation of fingerprint template. Pattern Recogn. Lett. **45**, 189–196 (2014)
6. Wang, S., Hu, J.: A blind system identification approach to cancelable fingerprint templates. Pattern Recogn. **54**, 14–22 (2016)
7. Wang, S., Deng, G., Hu, J.: A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. Pattern Recogn. **61**, 447–458 (2017)
8. Cappelli, R., Ferrara, M., Maltoni, D.: Minutia cylinder-code: a new representation and matching technique for fingerprint recognition. IEEE Trans. Pattern Anal. Mach. Intell. **32**(12), 2128–2141 (2010)
9. Ferrara, M., Maltoni, D., Cappelli, R.: Noninvertible minutia cylinder-code representation. IEEE Trans. Inf. Forensics Secur. **7**(6), 1727–1737 (2012)
10. Ferrara, M., Maltoni, D., Cappelli, R.: A two-factor protection scheme for MCC fingerprint templates. In: International Conference of the Biometrics Special Interest Group, pp. 1–8 (2014)
11. Abraham, J., Gao, J., Kwan, P.: Fingerprint matching using a hybrid shape and orientation descriptor. INTECH Open Access Publisher (2011)
12. Fingerprint Verification Competition: FVC 2002 database. http://bias.csr.unibo.it/fvc2002/databases.asp
13. Boult, T.E., Scheirer, W.J., Woodworth, R.: Revocable fingerprint biotokens: accuracy and security analysis. In: IEEE International Conference on Computer Vision and Pattern Recognition, CVPR, pp. 1–8, June 2007