A Score-Level Fusion Method for Protecting Fingerprint and Palmprint Templates

Mulagala Sandhya, Y. Sreenivasa Rao, Sahoo Biswajeet, Vallabhadas Dilip Kumar, and Maurya Anup Kumar

1 Introduction

Biometric refers to our use to progress in the evaluation and examination of the physiological or behavioral properties of a person [1, 2]. However, uni-biometric frameworks which use only biometric characteristic for recognition often suffer negative results such as spoof attacks, lack of characteristics, low accuracy of recognition, and biometrics information variation [3]. A multi-biometric framework combines two or more springs with different biometric characteristics, such as fingerprint, palm print, face, iris, and finger vein, etc. [4]. We cannot reset or replace a compromised biometric template. An important protection template technique is cancelable biometrics, which performs a one-way transformation for verifying the original data [5]. Mathematically, this one-way processing cannot be inverted, and only changing transformation parameters can effectively revoke and replace this trading template. The accompanying four necessities that should be met by a legitimate model are diversity, revocability, irreversibility, and performance. Multimodal biometric fusion can be divided into two types: Fusion before matching and Fusion after matching. Fusion at the level of the sensor and the level of the features are essentially considered as fusion prior matching. Following matching, fusion at match score level and decision level can be fused [2]. The multi-biometric systems are the systems that use

M. Sandhya (✉) · S. Biswajeet · V. Dilip Kumar
Computer Science and Engineering, National Institute of Technology Warangal,
Warangal, India
e-mail: msandhya@nitw.ac.in

Y. Sreenivasa Rao
Department of Mathematics, National Institute of Technology Warangal, Warangal, India
e-mail: ysr@nitw.ac.in

M. Anup Kumar
Goa Institute of Management, Sanquelim, India
e-mail: anupmaurya88@gmail.com

P. Stănică et al. (eds.), *Security and Privacy*, Lecture Notes in Electrical Engineering 744,
https://doi.org/10.1007/978-981-33-6781-4_1

more than one physiological or behavioral characteristic. Generally, multi-biometric systems are classified as Multi-sensor systems, Multi-algorithmic systems, Multi-Instance systems, Multi-sample systems, and Multimodal systems. The multi-modal systems establish an identity based on the evidence of multiple biometric traits. These systems offer considerable rise in the accuracy of a biometric system.

1.1 T-Norm & T-Conorms

We now present a brief overview of the triangular norms and triangular conorms.
T-norm:
Definition: A function $T : [0, 1]^2 \rightarrow [0, 1]$ is known as *triangular norm (t-norm)* if it satisfies the following properties for all $a, b, c \ \epsilon \ [0, 1]$ [6]
(T1) $T(a, b) = T(b, a)$, i.e., the t-norm satisfies commutative property,
(T2) $T(T(a, b), c) = T(a, T(b, c))$, i.e., the t-norm satisfies associative property,
(T3) $a \leq b \rightarrow T(a, b) \leq T(b, c)$, i.e., the t-norm satisfies monotone property,
(T4) $T(a, 1) = a$, i.e.,1 is the neutral element.

T-conorm:
Definition: A function $S : [0, 1]^2 \rightarrow [0, 1]$ is called *triangular conorm(t-conorm)* if it satisfies the following properties for all $a, b, c \ \epsilon \ [0, 1]$ [6]
(T1) $S(a, b) = s(b, a)$, i.e., the t-conorm satisfies commutative property,
(T2) $S(s(a, b), c) = s(a, s(b, c))$, i.e., the t-conorm satisfies associative property,
(T3) $a \leq b \rightarrow S(a, b) \leq S(b, c)$, i.e., the t-conorm satisfies monotone property,
(T4) $S(a, 0) = a$, i.e., 0 is the neutral element.
The rest of the paper is organized as follows: Sect. 2 provides related work, Sect. 3 gives the proposed score-level fusion method. Section 4 gives experimental results and analysis of proposed method. Section 5 concludes the paper.

2 Related Work

Barrero et al. [7] proposed architecture for protecting multi-biometric templates using homomorphic encryption. Barrero et al. [8] proposed a fingerprint and finger vein based fusion mechanism using bloom filters. Sandhya and Prasad [9] proposed a method for fusing two algorithms at score level for fingerprint templates using triangular norms. Chang et al. [10] developed a new framework BIOFUSE by the combination of fuzzy commitment and fuzzy vault using the format-preserving encryption scheme. Chin et al. [11] proposed a technique to generate an integrated template of fingerprint and palmprint using random tiling and discretization. Sandhya and Prasad [12] provided a clear review of template protection schemes in the literature and provided various sources of available datasets for the ongoing research on template protection schemes carried out worldwide. Dinca and Hancke [13] provided a survey on fusion methods and security highlighting the open challenges in this area of research work. Multi-biometric Systems offer improved accuracy, fault tolerance, and resistance to spoofing, at the same time add complexity for developers in terms of gathering sample inputs and how the templates are used to decide the user is genuine or an imposter. Hence we proposed a method for fusing fingerprints and palmprints at score level thereby improving performance with added security.

3 Proposed Method

The proposed method for fusing fingerprint & palm print at score level contains the following steps as shown in Fig. 1. Minutiae are the most significant points present in the fingerprint which helps in deciding the uniqueness of a fingerprint. We extracted them using the Verifinger SDK tool.

3.1 Binary String Generation from Fingerprint Image

Let f_p be a fingerprint image, we extract a set of minutiae represented by (x, y, θ, δ), θ is the orientation of the point, and δ is the type of minutia, (x, y) is the x and y coordinate location. A local structure p_{jk} constructed by the pair of minutia formed in fingerprint image by matching each minutia with all other minutiae points. For instance, Fig. 2 shows minutia pair m_j and m_k. If m_j is paired with m_k to form p_{jk}, then symmetric minutia pair of p_{kj} is excluded to maintain a strategic distance without redundancy. Assume that in a fingerprint image f_p, there are N_1 minutiae; a group of $C_2^{N_1}$ minutiae pairs are built. The following are characterized for every pair, p_{jk} with translation and rotation-invariant properties.

- Edge length, for example, l_{jk}.
- Every minutia angle to the edge, for example, α_j and α_k.
- Generally each minutiae is of type δ_k and δ_j. Therefore, a overall total of $C_2^{N_1}$ characteristics such as $l_{jk}, \alpha_j, \alpha_k, \delta_j, \delta_k$ can be removed in fingerprint image f_p from minutia $C_2^{N_1}$ couples formed by N_1 Minutiae.
- For example consider an integer value 300 i.e. V_{jk}=300 then the 300th position of the set [0, 2¬Lf-1] is indexed by ‘1’ and remaining positions are indexed with ‘0’. Then we integrate all these binary strings into a single vector Bf which is of length 2Lf which is shown in Fig. 3.

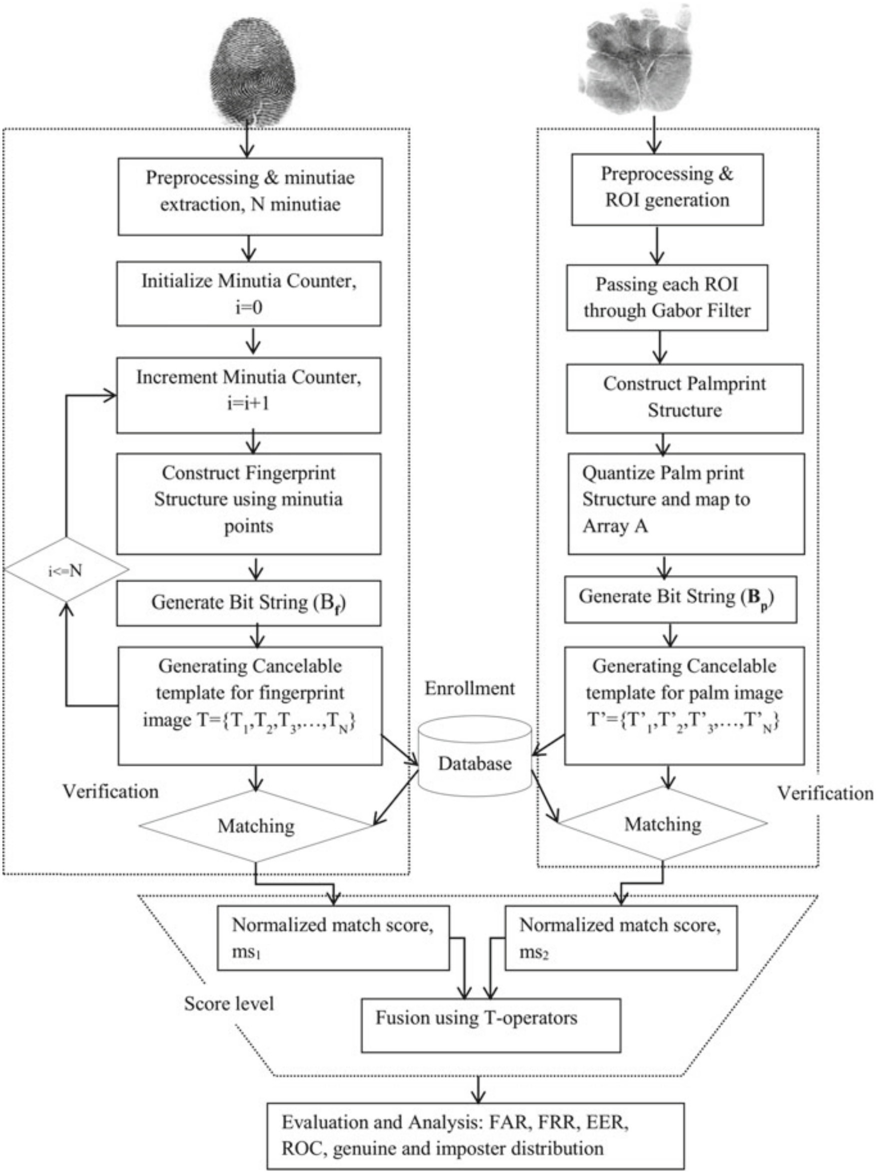

Preprocessing & minutiae extraction, N minutiae
Initialize Minutia Counter, i=0
Increment Minutia Counter, i=i+1
Construct Fingerprint Structure using minutia points
i<=N
Generate Bit String (B_f)
Generating Cancelable template for fingerprint image T={T_1,T_2,T_3,…,T_N}
Verification
Matching
Enrollment
Database
Preprocessing & ROI generation
Passing each ROI through Gabor Filter
Construct Palmprint Structure
Quantize Palm print Structure and map to Array A
Generate Bit String ($\mathbf{B}_p$)
Generating Cancelable template for palm image T'={T'$_1$,T'$_2$,T'$_3$,…,T'$_N$}
Verification
Matching
Normalized match score, ms_1
Normalized match score, ms_2
Score level
Fusion using T-operators
Evaluation and Analysis: FAR, FRR, EER, ROC, genuine and imposter distribution

Fig. 1 Flowchart of the proposed method

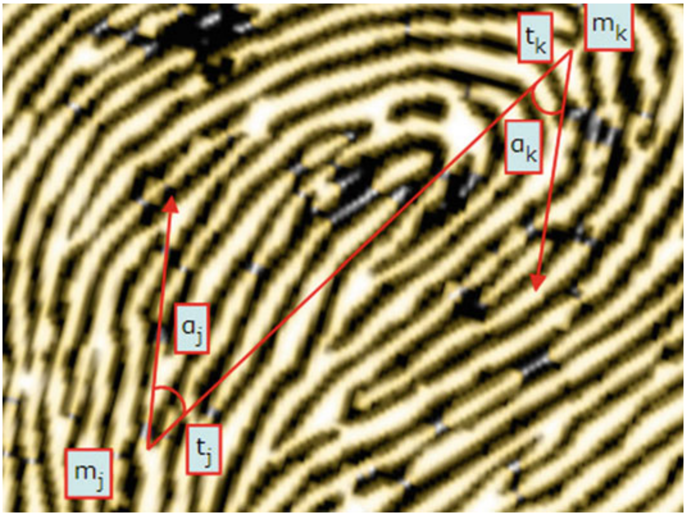


Fig. 2 Minutia pair p_{jk}—example of local minutia structure

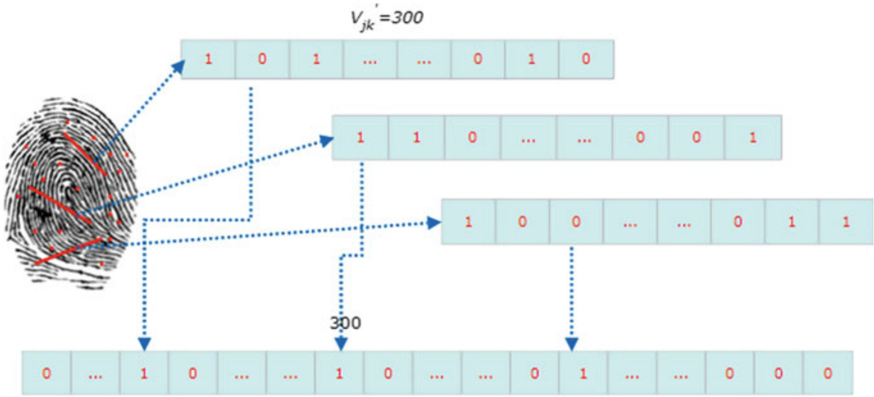


Fig. 3 Minutiae pair, a local minutia structure example

3.2 *Palm Print Feature Extraction and Transformation*

Passing ROI through Gabor filter

A Gabor filter, balanced by a Gaussian envelope is composed as

$$G(x, y, \sigma, \theta) = \frac{1}{2\pi\sigma^2}\, e^{-\dfrac{x^2 + y^2}{2\sigma^2}} e^{j2\pi(x\cos\theta + y\sin\theta)}$$

Algorithm 1 Generation of Finger print Match Score

```
Input:
Minutiae locations $(x_i, y_i)$
Orientation of minutiae points $\theta_i$
Total number of minutiae points $N$
Random matrix $R$
Output: Normalized match score
begin
Initialize minutiae counter $i \leftarrow 0$;
$N \leftarrow$ Number of minutiae points in a fingerprint image;
while $i \leq N$ do
    for each j $\leftarrow N - 1$ points
     $l_{ij}$: Length of the edge
     $\alpha_i$ and $\alpha_j$ : Angle between orientation of each minutiae and edge
     $\delta_i$ and $\delta_j$ : Type of each Minutiae
     $V_{ij} \leftarrow l_{ij}||\alpha_i||\alpha_j||\delta_i||\delta_j$, which contains $L_f = L_1 + L_2 + L_3$ +2;
     $L_f$ bits represents $2^{L_f}$ ranging from 0 to $2^{L_f}$-1 to get $B_f$ binary vector
end while
while $i \leq Size(B_f)$ do
     $V \leftarrow DFT(B_f)$;
     $T(i) \leftarrow R \times V$;
     $i \leftarrow i + 1$;
end while
Match score $ms_1$ generation;
end
```

where θ and σ signify the orientation of Gabor filter and bandwidth, respectively, and $j = \sqrt{-1}$. We use the palmprint images filtered by Gabor. Wavelengths are considered orientations $\theta = \{0, 90\}$ and $\sigma = \{5, 10\}$, resulting in four filters from Gabor and for each ROI, a phased image is provided. After plotting the graph concerning phase and magnitude, we can convert the graph into a 2-D matrix and then convert the 2-D matrix into a 1-D vector to get B_p. Certain quantization steps can be used for the graph to convert it into a 2-D matrix. The palmprint feature vector B_p is bolstered non-invertible transformation based on the DFT that produces an identical feature-length vector of B_p.

Cancelable template generation

Let the bit string length B_p be m. n^1-point discrete fourier transformation is applied to B_p. Complex vector V^1 is produced as follows [9]

$$V' = \sum_{s=0}^{n^1-1} B_p e^{-\frac{j2\pi is}{n'}}, \qquad i = 0, 1, \ldots, n^1 - 1$$

Thus, the size of V^1 is $n^1 \times 1$. A random matrix (R) of dimension $m \times n^1$ for V^1 is generated. To obtain T^1, we multiply R^1 and V^1, where T^1 is the template that can be cancelable. Thus the size of T^1 is $m \times 1$.

$$R'_{m\times n} \times V'_{n\times 1} = T'_{m\times 1}$$

In addition, we create N canceled vector templates in $T^1 = (T_1, T_2, \ldots, T_N)$ representing palm print, where N is the number of canceled vector templates.

Algorithm 2 Generation of Palm Print Match Score

```
Input:
ROI of palmprint $I$
Random matrix $R$
Output: Normalized match score
begin
Input ROI's $I$ to Gabor Filter to get a graph between phase and magnitude
Convert the Graph into 2-D binary matrix
Convert 2-D matrix to 1-D binary vector $B_p$
while $i \leq Size(B_p)$ do
    $V' \leftarrow DFT(B_p)$;
    $T'(i) \leftarrow R' \times V'$;
    $i \leftarrow i + 1$;
end while
Match score $ms_2$ generation;
```

3.3 Score-Level Fusion

Table 1, where p covering the T-operative space, which is indicated by the T-conorms implemented in our fusion method [9].

Table 1 Fusion of match scores of fingerprint and palmprint implemented using T-conorms

S.No.	T-conorm	S(S_1,S_2)
1.	Zadeh (max rule)	$\max(S_1, S_2)$
2.	Goguen, Bandler	$S_1 + S_2 - S_1.S_2$
3.	Dombi ($0 < p < +\infty$)	$\frac{1}{1+((\frac{1-S_1}{S_2})^{-p}+(\frac{1-S_2}{S_2})^{-p})^{-\frac{1}{p}}}$
4.	Dubois ($p\epsilon[0, 1]$)	$1 - \frac{(1-S_1)(1-S_2)}{\max(1-S_1, 1-S_2, p)}$
5.	Sugeno-Weber ($(-1 < p < +\infty)$)	$\min(S_1 + S_2 + p.S_1.S_2, 1)$
6.	Yu Yandong ($(-1 < p < +\infty)$)	$\min(S_1 + S_2 + p.S_1.S_2, 1)$

3.4 Transformed Domain Matching

Let, Y^T be the feature vector of the template and Y^Q be the feature vector of query (T and Q superscripts mean template and query, respectively). The Y^T and Y^Q are both complex vectors. The similarity is calculated using the following equation:

$$S(Y^T, Y^Q) = 1 - \frac{||Y^T - Y^Q||_2}{||Y^T||_2 + ||Y^Q||_2} \tag{1}$$

where $|| \cdot ||_2$ represents the 2-norm. The similarity scores $S(Y^T, Y^Q)$ is in the range [0, 1]. The greater the score of similarity, the template, and query feature vectors are similar.

4 Experimental Results & Analysis

4.1 Experimental Setup

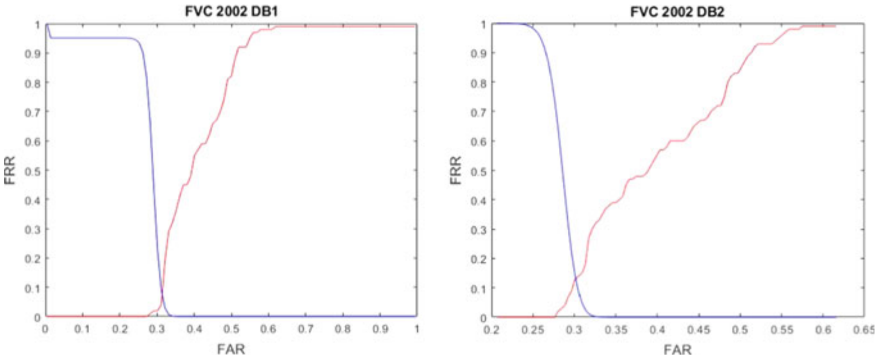
To test the proposed method, we used databases FVC 2002 (DB1, DB2) for fingerprints and HandV2 for palmprint images.

4.2 Accuracy

Two cases will be considered to assess the accuracy of our proposed fusion method. First, when each user is assigned a different key, i.e., each user is assigned a specific key that is unique to each user. This process is referred to as plain verification. The EER value for this scenario is ideal, i.e., for all two FVC 2002 DB1 and FVC 2002 DB2, it shows the EER as 0%. Second, stolen or lost key, where the attacker has the key of the user and he is trying to verify. The EER value for this scenario is greater than 0, like in the case of FVC 2002 DB1 is 6.58% & for FVC 2002 DB2 is 9.95%. Figures 4a, b represent EER values of the proposed method.

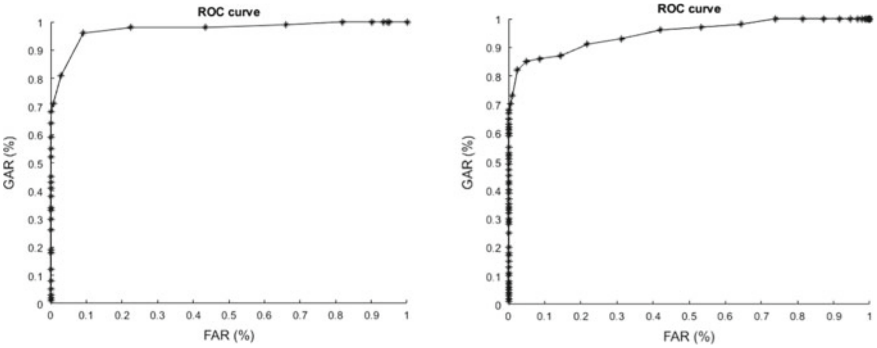
The ROC curve for the proposed fusion method is shown in Fig. 5a, b for FVC 2002 DB1 and DB2, respectively.

Table 2 represents the EER reported for the proposed method by using score-level fusion of the match scores using T-norms by fusing FVC DB1 and DB2 databases. with Handv2 databases. We have run the two types of fusion mechanism for 200 samples (100 users) on FVC 2002 DB1 and DB2 where Score level Fusion is giving better results compared to Feature-Level Fusion, i.e., the lowest EER we are achieving is for FVC 2002 DB1 which is 6.58%.



(a) EER value of FVC 2002 DB1 (b) EER value of FVC 2002 DB2

Fig. 4 **a** EER value of FVC 2002 DB1. **b** EER value of FVC 2002 DB2



(a) ROC Curve of FVC 2002 DB1 (b) ROC Curve of FVC 2002 DB2

Fig. 5 **a** ROC Curve of FVC 2002 DB1. **b** ROC Curve of FVC 2002 DB2

Table 2 EER values against different fusion methods

Samples(N)	Fusion method used	$EER(\%)$ for FVC 2002 DB	
		DB1	DB2
200	Feature-level fusion	36.5	37.03
200	Score-level fusion	6.58	9.95

4.3 Security Analysis

Consider the following cases for security analysis:

- *Inverse attack*: For each fingerprint image, all minutiae are considered, where each minutia has a different position, orientation with respect to other minutiae which makes it difficult to generate the binary vector. Here, it's hard to reconstruct B_f and B_p.

- *Non-invertibility*: Non-invertibility claims that it is almost impossible to construct an original fingerprint image & palm-print image from the transformed template. By using the help of DFT and multiplying with the random matrix, we can provide one-way functionality to our template. Hence making our solution secure.

5 Conclusion and Future Scope

We have used Fingerprint and Palmprint as the multi-biometric traits and used minutiae position and Gabor filter, respectively, for generating binary vectors. In this method, we are not directly storing distance between minutia, orientation, type, etc., for fingerprint and phase and magnitude for palmprint. But we are storing the attributes such that if any template got leaked the information like distance between two minutia points, orientation will not be revealed directly to the attacker. Then we used DFT to create a cancelable template for each of the vectors and then calculate the match score for both the respective vectors. The match score for both the vectors are fused using the T-operators to give the resultant match score.

References

1. Jain AK, Nandakumar K, Nagar A (2008) Biometric template security. EURASIP J Adv Signal Process 113
2. Ross A, Govindarajan R (2004) Feature level fusion in biometric systems. In: Proceedings of the 2004 biometric consortium conference, p 2
3. Rathgeb C, Gomez-Barrero M, Busch C, Galbally J, Fierrez J (2015) Towards cance-lable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In: Proceedings of the 2015 international workshop on biometrics and forensics (IWBF), pp 1-6
4. Jagadeesan A, Duraiswamy K (2010) Secured cryptographic key generation from multimodal biometrics: feature level fusion of fingerprint and iris. Int J Comput Sci Inf Secur 7:28–37
5. Lin K, Han F, Yang Y, Zhang Z (2011) Feature level fusion of fingerprint and finger vein biometrics. Adv Swarm Intell 6729:348–355
6. Ratha N, Chikkerur S, Connell J, Bolle R, Generating cancelable fingerprint templates. IEEE Trans Pattern Anal Mach Intell 29(4):561–572
7. Gomez-Barrero M, Maiorana E, Galbally J, Campisi P, Fierrez J (2017) Multi-biometric template protection based on homomorphic encryption. Pattern Recognit 67:149–163
8. Gomez-Barrero M, Rathgeb C, Li G, Ramachandra R, Galbally J, Busch C (2018) Multi-biometric template protection based on bloom filters. Inf Fusion 42:37–50
9. Sandhya M, Prasad MVNK, Multi-algorithmic cancelable fingerprint template generation based on weighted sum rule and T-operators. Pattern Anal Appl 21:397–412
10. Chang D, Garg S, Ghosh M, Hasan M (2021) BIOFUSE: a framework for multi-biometric fusion on biocryptosystem level. Inf Sci 546:481–511
11. Chin YJ, Ong TS, Teoh ABJ, Goh KOM (2014) Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Inf Fusion 18:161–174

12. Sandhya M, Prasad MVNK (2017) Biometric template protection: a systematic literature review of approaches and modalities. In: Jiang R, Al-maadeed S, Bouridane A, Crookes P, Beghdadi A (eds) Biometric security and privacy. Signal Processing for Security Technologies, Springer, Cham
13. Dinca LM, Hancke GP (2017) The fall of one, the rise of many: a survey on multi-biometric fusion methods. IEEE Access 5:6247–6289