The Visual Computer (2021) 37:1401–1413
https://doi.org/10.1007/s00371-020-01873-x

ORIGINAL ARTICLE

Novel approach for multimodal feature fusion to generate cancelable biometric

Keshav Gupta[1] · Gurjit Singh Walia[2] · Kapil Sharma[3]

Published online: 13 June 2020

Abstract

Biometric systems provide various benefits over traditional pin-based authentication systems. However, the issue of data privacy and theft is of great concern. To resolve these issues, a novel cancelable multimodal biometric system is proposed that combines multiple traits by means of a projection-based approach. The proposed approach generates a cancelable biometric feature that is used to obtain revocable and noninvertible templates. Cancelable features are generated by projecting the feature points onto a random plane obtained using a user-specific key. The point of projection is then transformed into cylindrical coordinates and a combined cancelable feature is obtained. Extensive experiments are performed over 3 chimeric multimodal databases and results reveal high performance. The average DI and EER achieved by the proposed method are 16.63 and 0.004, respectively. Also, the proposed method is successfully analyzed for privacy concerns, namely revocability, non-invertibility, and unlinkability. Moreover, the proposed system demonstrated tolerance against various security attacks like brute force attacks, attacks via record multiplicity, and substitution attacks.

Keywords Cancelable template · Feature fusion · Multimodal biometric

1 Introduction

Biometric authentication systems are gaining high popularity and public acceptance due to a wide variety of uses. It includes identification, authentication, forensics, and access control. With the increase in usage, the number of threats and attacks like spoofing attacks, template thefts, etc. are also increasing. Thus, securing the biometric system itself is a challenge as biometric data for an individual is irreplaceable. If it is compromised, then it cannot be changed or replaced making its protection a very crucial task.

To overcome problems such as spoof attacks, poor input data quality, non-universality, etc. multimodal biometric systems came into existence [1]. Here, information from complementary and fairly independent modalities was fused to reach a final decision [2]. This fusion process may take place at the feature level, score level, decision level, sensor level, and rank level. In feature level fusion, extracted features from various biometric modalities are fused to generate a more discriminative feature. On the other hand, matching score values from multiple classifiers is combined in score level fusion [3]. At decision level fusion, results from different classifiers are combined together using methods like majority voting [2, 4]. Fusion at feature level generally provides better results as compared to other fusion techniques since the information available about biometric data is very high at this level [4, 5]. But to achieve fusion at feature level is strenuous as in many cases the features are not compatible. Generally, multimodal systems are very helpful in dealing with above-stated issues but no protection is available for biometric data itself in case of template hacking or database stealing. The security of biometric data should be of top priority as biometric information cannot be replaced easily. If biometric templates are stolen, the user's identity

✉ Kapil Sharma
kapil@ieee.org

Keshav Gupta
keshavgupta101@gmail.com

Gurjit Singh Walia
gurjit.walia@gmail.com

[1] Department of Computer Science, Delhi Technological University, New Delhi, India

[2] SAG, Defence Research and Development Organization, New Delhi, India

[3] Department of Information Technology, Delhi Technological University, New Delhi, India

is compromised for multiple applications and subject to cross-application attacks as well. Overall, it not only threatens the security, but it may also incur a significant financial or social loss. To resolve these issues, cancelable biometrics is widely used.

Cancelable biometric systems use a pseudo-biometric template instead of the original template for matching and verification purposes. These pseudo-templates are generated from original templates using various transformation mechanisms. For instance, in non-invertible geometric transformations, a feature domain transformation is applied using transformation techniques such as Cartesian, polar and functional transformation [6]. Random projection is also used as a non-invertible transformation [7, 8] wherein an extracted feature $x \in F_n$ is projected to a random subspace $Y \in F_n \times N$ with $n < N$ and all element of y are independently realized from a random variable as $z = Yx$ where z is random projection vector. A random convolution method was proposed in [9] to produce cancelable templates wherein a user-specific kernel is used to encrypt the biometric data. Bio-convolving is also a convolution-based approach for generating cancelable templates [10]. In this, biometric template was segmented into various sequences and a transformed sequence is generated using linear convolution. An extension of random projection is bio-hashing [11] wherein a bio-hash template was generated using a user-specific random number. Random permutation of features is also been used by many researchers for generating cancelable templates [12]. There are also various salting methods where a random pattern or noise is mixed with the original template. The techniques used for the cancelable biometric template must exhibit properties, viz. revocability, security, diversity, and accuracy. Recently, researchers are also working at hybrid methods where more than one technique is used to generate cancelable templates.

In the proposed work, a multimodal biometric system is introduced using two complementary biometric traits, viz. fingerprint and iris where complementary information is fused using feature-level fusion. The proposed system is highly secure as well as tolerant of template hacking by means of cancelable templates. Cancelable templates are generated using a novel transformation technique where the feature vectors from two modalities are used to generate abscissa and ordinate of a feature point. These feature points are orthogonally projected on a random plane generated using a user-specific key. The projected point is then transformed into a cylindrical coordinate system to receive θ, ρ, z values. In the next step, θ values for every feature point are combined together to generate a transformed template which is irreversible in nature. The proposed method is faster, cheaper and provides high performance. Also, the cancelable templates generated are non-invertible, revocable and diverse in nature. The proposed method is evaluated on multimodal chimeric datasets obtained from benchmarked images. A brief summary of the proposed work is discussed as follows:

- A novel multimodal biometric system using two complementary features, namely fingerprint and iris is proposed. A cancelable biometric template feature is generated by combining the information from these traits.
- Cancelable biometric templates are generated from the feature vectors of the modalities using a user-specific random key set. Here, the feature points from the corresponding feature vectors used as abscissa and ordinate are projected on a random plane that is generated using a user-specific random key set.
- The point of projection on a random plane is transformed into a cylindrical coordinate system to generate r, θ, z values. A different plane is generated for each feature point to generate unique points of projection. From every point, θ values are combined together to generate cancelable template.
- The proposed method is evaluated over three multimodal chimeric datasets created using benchmarked images. The results reveals high performance, high privacy, high security and low error rate compared to state-of-the-art techniques.

The rest of the manuscript is arranged in the following manner: In Sect. 2, various state-of-the-art methods for generating cancelable templates and feature-fusion techniques are discussed and compared. In Sect. 3, details of the proposed biometric system are discussed at length. Section 4 contains the experimental validation, database design and performance analysis of the proposed method. Finally, Sect. 5 contains the conclusion and future scope of the work done.

2 Related work

Cancelable biometrics is used to protect templates by performing the matching and storage in a different domain [13]. Generally, in the case of template stealing, the stolen template is revoked and an entirely different template is created by altering the key. Thus, it fulfills the necessary requirements for template protections, namely revocability, non-invertibility, diversity and accuracy [13, 14]. Transformation performed on biometric data can be mainly classified as non-invertible transforms and biometric salting. Biometric salting can be additionally classified as projection-based transformations, noise-based transformation, and convolution-based transformation.

Transformations based on random projection projects biometric data to a random sub-space using various transformation techniques. The most popular technique in this category is bio-hashing [11] which projects the features into the orthonormal sub-space. It provides good discrimination capability and high performance. However, this method suffers from the problem of irreversibility if both template and transformation matrix are compromised. In [15], authors proposed an extension of the bio-hash technique to address the issue of stolen-token scenarios. In this, the authors used a novel multi-state discretization technique instead of a simple threshold scheme. Pillai et al. proposed a new variant of random projection, namely Sectored random projection [7] technique where the biometric feature is segmented into various sectors, then on each sector, the random projection is applied and concatenation was performed to generate the cancelable template. This method not only caters to the issue of useful iris area reduction, but it is also robust to common iris outliers. To improve non-invertibility, Teoh et al. [16] introduced a novel technique, random multi-space quantization (RMQ), wherein the biometric feature vector was mapped with a sequence of random sub-spaces using a pseudo-random sequence. In the second step, quantization was performed based on a threshold value. Teoh et al. also proposed a multi-space random projections technique [17] which is a two-factor cancelable formulation and feature vector obtained from biometric modalities is projected to multiple random subspaces based on a user-specific pseudo-random number. Wang et al. proposed a random projection with vector translation method [18] for cancelable biometrics wherein biometric data was projected using a Gaussian random variable. Also, Paul et al. [19] proposed a random cross-folding method using random projection and selection to create cancelable templates. In order to make it a user-dependent dynamic process, Yang et al. proposed a nonlinear projection process in which the projection vector was dynamically decided by feature vector itself [20]. In general, most of the projection techniques discussed are vulnerable to attacks such as inverse operations if both templates and transformation matrix are stolen [21]. Accordingly, researchers have proposed other methods like random convolution transformations for generating cancelable templates.

In random convolution (RC) based transformations, cancelable templates are generated by convolving the biometric feature using a random kernel. Savvides et al. [9] used minimum average correlation energy (MACE) filters as a convolution method to generate cancelable templates. In [22], authors used the concept of locality sensitive hashing to generate secure, cancelable iris features. Maiorana et al. proposed a bio-convolving technique where a set of non-invertible transformations were performed on sequence-based biometric representation [10]. But if kernel used for transformation is known, it can be vulnerable to inverse attacks. To overcome this issue, an algorithm using curtailed circular convolution was proposed [23]. The algorithm convolved input binary features in a circular manner using random binary strings imparting non-invertibility. In [24], the authors used the quality of fingerprint features to determine the presence of live fingerprint. Similarly, Ali et al. [25] used a user key set to modify minutiae information from fingerprint to produce cancelable templates. Further, Trivedi et al. [26] used a binary user key on fingerprint modality to generate cancelable templates. On the other hand, Wu et al. [27] presented ECG as a biometric and generated revocable templates using signal subspace collapsing. The cancelable biometrics is also widely used with multimodal biometric systems to remove various limitations imposed by unimodal systems.

Rathgeb and Busch used adaptive bloom filters to transform iris feature for both eyes of a single subject and fused them at feature level [28]. This method provided improved performance but vulnerable to template linking. A random permutation principal component analysis (RP-PCA) method was introduced by Kumar et al. [29] to generate cancelable biometric using face, iris, and ear modality. The accuracy of the system was unaffected, and the robustness of the system was improved. Also, Dwivedi and Dey [30] created a hybrid scheme for a cancelable multi-biometric system combining mean-closure weighting (MCW) with Dempster-Shafer (DS) theory. This scheme showed robustness against score variability and considerable performance improvement over uni-modal counterparts. Similarly, Walia et al. [31] proposed a cancelable biometric system by performing cross-diffusion of graphs. Later, PCR-6 was used to fuse belief masses from individual classifiers. Experimental results demonstrated better performance than many existing techniques. Kaur and Khanna [32] proposed a novel random distance technique for transformation in a multi-biometric scenario using face, palmprint, and finger-vein as input modalities. Similarly, walia et al. [33] used key images to generate cancelable features and dimension reduction. A multifold random projection was introduced by Paul and Gavrilova [34] for a multimodal biometric system with improved recognition performance. Chin et al. [35] proposed a template protection scheme wherein original fingerprint and palmprint templates were arranged in random rectangles using user-specific keys. Later, statistical features were extracted and fused at the feature level to generate cancelable templates. Similarly, Gomez-Barrero et al. [36] used bloom filters on face-finger vein and face-iris to generate protected templates and a weighted feature level fusion was performed to generate the multimodal cancelable template. With increasing attacks on biometric systems, detection of fake biometric is equally important as the protection of biometric data.

Recently, deep learning methods are widely used for feature representation. For instance, Essam et al. [37] identified various regions in face image using multiple CNNs. Later, bio-convolving encryption was used to generate cancelable templates. Also, Das et al. [38] proposed a finger-vein identification method based on deep learning. Similarly, in [39], a novel architecture ScoreNet was introduced for unconstrained ear recognition wherein deep learning and hand-crafted methods were used together. Further, Liu et al. [40] presented a detailed discussion about various deep learning methods for feature representation.

Based on the above discussion, it is evident that securing biometric systems from various attacks should be of top priority. Accordingly, a multimodal biometric system with cancelable templates and liveness detection is proposed in this manuscript which complements the advantages of various techniques and improves the overall performance of the biometric system. A detailed explanation of the proposed methodology is provided in the next section.

3 Proposed multimodal cancelable biometric system

Figure 1 represents the architecture of the proposed system. In this, a cancelable template is generated for Iris(i) and Fingerprint(p) features using the proposed technique with user-specific keys.

The proposed cancelable biometric system takes two biometric modalities, viz. iris and fingerprint and feature vectors are extracted. For extracting features from iris modality, image pre-processing combined with local binary pattern (LBP) [41] is performed [42]. LBP not only provides low computation but also immune to changes in image grey levels. For fingerprint modality, the input query image is preprocessed by performing binarization and thinning operations. Next, feature extraction is performed to generate minutiae-based features from the input image.

Feature points at *i*th position of the iris feature vector is considered as abscissa and fingerprint feature as ordinate. Combining them together, a point (χ_i, ψ_i) is defined in a cartesian coordinate system. Each point thus obtained is projected onto a plane corresponding to each feature point obtained using a user-specific key. The points of projection thus obtained are transformed into a cylindrical space to obtain corresponding feature points. The azimuth values are considered for generating cancelable templates so as to achieve non-invertibility. A similarity score is calculated by matching the generated feature with the stored templates in the database. Finally, the match score is compared with an optimal threshold value to reach a final decision. The proposed system is non-invertible in nature as only the azimuth values are considered for generating the cancelable templates. The in-depth details of the proposed system are presented in the next subsection.

3.1 Multimodal feature extraction

Biometric modalities, viz. iris and fingerprint are processed using feature extraction techniques to determine individual feature vectors. For fingerprint features are extracted using a minutiae-based technique which is widely used by researchers [43, 44] as it provides low complexity with high performance. For this, first of all, binarization and thinning operations are performed as a pre-processing step on input query

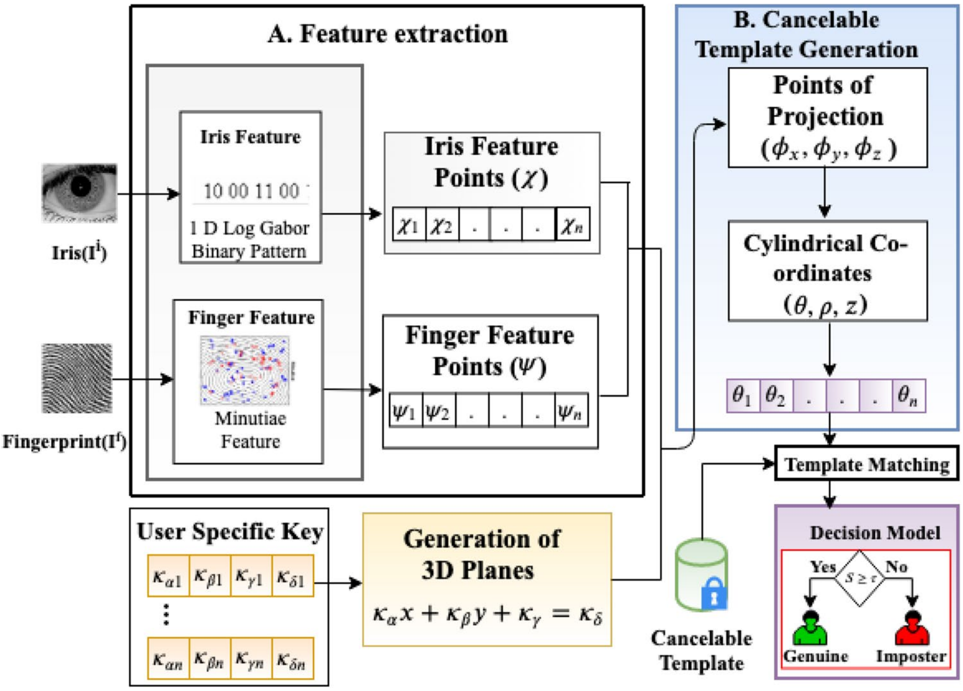

A. Feature extraction
Iris Feature
10 00 11 00
1 D Log Gabor Binary Pattern
Iris(I^i)
Finger Feature
Minutiae Feature
Fingerprint(I^f)
Iris Feature Points (χ)
χ_1 χ_2 . . . χ_n
Finger Feature Points (ψ)
ψ_1 ψ_2 . . . ψ_n
B. Cancelable Template Generation
Points of Projection (ϕ_x, ϕ_y, ϕ_z)
Cylindrical Co-ordinates (θ, ρ, z)
θ_1 θ_2 . . . θ_n
Template Matching
Decision Model
Yes
$S \geq \tau$
No
Genuine
Imposter
User Specific Key
$\kappa_{\alpha 1}$ $\kappa_{\beta 1}$ $\kappa_{\gamma 1}$ $\kappa_{\delta 1}$
$\kappa_{\alpha n}$ $\kappa_{\beta n}$ $\kappa_{\gamma n}$ $\kappa_{\delta n}$
Generation of 3D Planes
$\kappa_\alpha x + \kappa_\beta y + \kappa_\gamma = \kappa_\delta$
Cancelable Template

Fig. 1 Overview of the proposed cancelable template generation scheme. Extracted features from the input query image are projected onto a plane obtained using a user-specific key. The points of projection are transformed into cylindrical coordinates to generate cancelable templates. These are compared with stored templates to evaluate similarity score to reach a final decision

fingerprint image I^f. Binarization operation helps in increasing the contrast between ridges and valleys as shown in Eq. 1

$$B(x,y) = \left\{ \begin{array}{ll} 1, & \text{if } I(x,y) \geq \ h \\ 0, & \text{otherwise} \end{array} \right\} \tag{1}$$

where $I(x,y)$ shows intensity value at pixel position (m,n) and h represents the value of threshold. Also, a thinning operation is used to reduce ridges to the unit-pixel thickness and is carried out using in-built morphological functions in the MATLAB platform on binary images. Rutovitz crossing number (CN) is computed by locating the minutiae over the thinned image using a sliding window of size 3×3 in an anti-clockwise manner [44]. The CN defines the minutia type and is calculated using Eq. 2

$$\text{CN} = \frac{1}{2}\sum_{k=1}^{8} |p_k - p_{k-1}| \tag{2}$$

where p_k is the pixel values of immediate neighbors for pixel k. The value of CN is used to classify ridge pixel as isolated, continuing, ending, crossing point and bifurcation. Further, minutia is represented as a vector $m = [x, y, \text{CN}, \theta]$ having (x, y) as the pixel coordinates and θ as angle of orientation. For input fingerprint query image I^f, an extracted feature vector, η^f is created by combining n minutiae using Eq. 3

$$\eta^f = [m_1, m_2, \dots m_n] \tag{3}$$

For iris feature extraction, input iris image I_i is pre-processed involving localization and normalization processes. In the first step, an integro-differential operator is used for localizing iris and pupillary boundaries. In the second step, Daugman's rubber sheet model [45] is used to normalize the localized iris into a fixed-sized rectangular block. Further, the processed image is quantified using the histogram of LBP. From LBP histogram values $l_1, l_2 \dots l_n$, feature vector for iris η^i is generated using Eq. 4

$$\eta^i = (l_1, l_2 \dots \dots l_n) \tag{4}$$

This creates a unique pattern, generating iris feature η^i. The extracted feature vectors η^i and η^f are fused together using the proposed method to generate a cancelable feature which is discussed in the next subsection.

3.2 Proposed multimodal feature fusion

The fusion process is very important in a multimodal biometric system for making a decision. Here, we have proposed a feature level fusion method with template protection. The proposed method generates a cancelable template which is revocable, non-invertible and robust to various types of attacks such that true biometric feature will not be revealed to the attacker. Every user is provided with a complex unique key (κ^k), where $k \in [1, N]$ used to create random 3-D planes as shown in Eq. 5.

$$\kappa^k = \begin{bmatrix} \kappa^k_{\alpha 1} & \kappa^k_{\beta 1} & \kappa^k_{\gamma 1} & \kappa^k_{\delta 1} \\ \kappa^k_{\alpha 2} & \kappa^k_{\beta 2} & \kappa^k_{\gamma 2} & \kappa^k_{\delta 2} \\ . & . & . & . \\ \kappa^k_{\alpha n} & \kappa^k_{\beta n} & \kappa^k_{\gamma n} & \kappa^k_{\delta n} \end{bmatrix} \tag{5}$$

Here, k represents the kth user. The length of the key is equivalent to the length of feature vectors and consists of n rows containing 4 co-efficient values namely $\kappa^k_{\alpha i}$, $\kappa^k_{\beta i}$, $\kappa^k_{\gamma i}$, and $\kappa^k_{\delta i}$ where $i \in [1, n]$ and having values randomly distributed in the range $[-1000, 1000]$. The user key is used to generate a random plane defined using Eq. 6 for each feature point as shown above in Fig. 1

$$\kappa_{\alpha i} x + \kappa_{\beta i} y + \kappa_{\gamma i} z = \kappa_{\delta i} \tag{6}$$

where $i \in [1, n]$. The random planes generated using user-specific keys are used in combining multiple features using the proposed approach. In this, feature vectors obtained during the feature extraction process are fused together by means of the proposed projection-based approach. Each feature point of the iris feature vector is considered as abscissa and each feature point of the fingerprint feature vector is considered as ordinate in a cartesian coordinate system. In case of different feature size, padding can be used so that every feature vector contain an equal number of feature points. Moreover, the abscissa and ordinates at the corresponding positions are combined to describe a point(Q) (χ, ψ) such that any user can be defined as in Eq. 7.

$$\upsilon = \left[(\chi_1, \psi_1) \ (\chi_2, \psi_2) \ (\chi_3, \psi_3) \ . \ . \ (\chi_n, \psi_n) \right] \tag{7}$$

For simplicity, the above equation can also be represented as shown in Eq. 8

$$\upsilon = \left[Q_1 \ Q_2 \ Q_3 \ . \ . \ Q_n \right] \tag{8}$$

Also, as discussed above, each user is provided with a unique user-specific key (κ^k) of dimension $4 \times n$. The key is used to create a different random plane corresponding to each point Q. Further, an orthogonal projection is performed from each of these points(Q) on the corresponding plane and point of projection(P) is obtained as shown in Fig. 2

For k^Pth user, each orthogonal projection from point $Q^k_i(\chi, \psi)$ on the random planes obtained using key κ^k generates a point $P^k_i(\phi_x, \phi_y, \phi_z)$ as in Eq. 9.

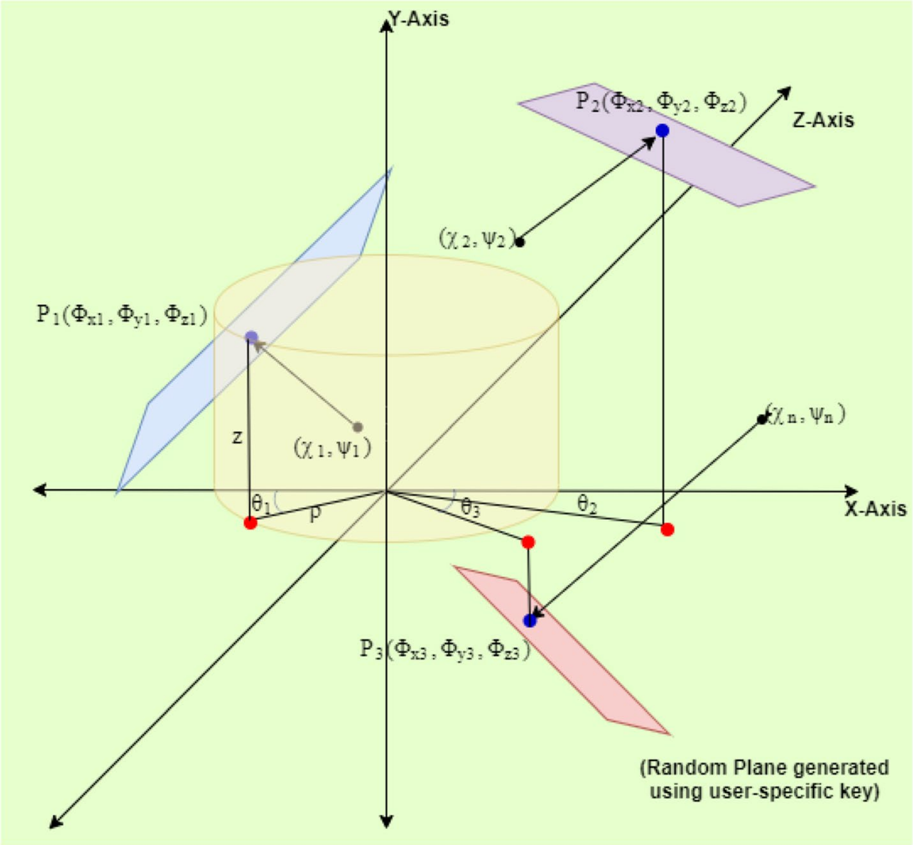


Fig. 2 Projection of feature points on random planes

$$\left[P_1^k \quad P_2^k \quad . \quad . \quad P_n^k\right] = \left[(Q_1^k \quad Q_2^k \quad . \quad . \quad Q_n^k\right] \begin{bmatrix} \kappa_{\alpha 1}^k & \kappa_{\beta 1}^k & \kappa_{\gamma 1}^k & \kappa_{\delta 1}^k \\ \kappa_{\alpha 2}^k & \kappa_{\beta 2}^k & \kappa_{\gamma 2}^k & \kappa_{\delta 2}^k \\ . & . & . & . \\ \kappa_{\alpha n}^k & \kappa_{\beta n}^k & \kappa_{\gamma n}^k & \kappa_{\delta n}^k \end{bmatrix} \tag{9}$$

In the next step, each point of projection (P_i^k) is transformed into cylindrical co-ordinates using a function f defined as in Eq. 10

$$P_i^k(\theta, \rho, z) = f(P_i^k(\phi_x, \phi_y, \phi_z)) \tag{10}$$

where ρ and θ are determined using Eqs. 11 and 12, respectively.

$$\rho = \sqrt{{\phi_x}^2 + {\phi_y}^2} \tag{11}$$

$$\theta = \tan^{-1} \frac{\phi_y}{\phi_x} \tag{12}$$

In the cylindrical coordinate system, point P is represented as θ, ρ, z. In the last step, the azimuth(θ) values corresponding to each point of projection(P_i^k) for kth user, are concatenated together to generate a fused vector ζ^k that is cancelable and non-invertible in nature as shown in Eq. 13.

$$\zeta^k = (\theta_1, \theta_2, \theta_3, \dots \theta_n) \tag{13}$$

The purpose of conversion to a 3D cylindrical coordinate system is to provide a higher dropout ratio as compared to the 2D coordinate system. Since only azimuth values are used to generate the cancelable template, a dropout ratio of 66.6% is achieved. On the other hand, a 2D point of projection would have led to a dropout ratio of 50% only. Further, in case of template theft, if azimuth (θ) values are compromised, it will lead to ambiguous values of ϕ_x and ϕ_y as evident from equation 12 and original feature points will not be exposed. Thus, the generated template is highly non-invertible and robust against theft. Also, the feature vectors from both Iris and Fingerprint modality of dimension $1 \times n$ are combined and converted into a single vector of dimension $1 \times n$. The cancelable feature obtained is compared with the stored templates to generate a final match score (S). The final decision is performed based on an optimal threshold value (τ), if the match score (S) is greater than τ, then it is considered as Genuine else imposter. The next section provides details of the experimental validation of the proposed method.

4 Experimental validation

The experimental validation of the proposed multimodal biometric system is performed over three multimodal chimeric databases. During privacy analysis, the proposed system is analyzed for unlinkability, non-invertibility, and revocability. Also, the system is analyzed for various attacks like record multiplicity, substitution, and brute force attacks to establish the robustness of the system. On the other hand, various performance metrics like equal error rate (EER), decidability index (DI), and recognition index (RI) are determined to estimate the system's performance. Also, the proposed system's performance is compared with other state-of-the-art methods.

4.1 Database and experimental design

The multimodal datasets are obtained using images from various benchmark datasets for experimental validation. Here, the Chimeric datasets are created by uniquely combining benchmark datasets, namely MCYT bimodal database [46], IITD PolyU iris database [47], Casia iris database (Casia-IrisV1, http://biometrics.idealtest.org/), FVC2006 DB1-A fingerprint database [48], and MMU2 iris database [49]. Sample images from the mentioned benchmarked datasets are shown in Fig. 3.

MCYT fingerprint database contains images captured using two different sensors, namely CMOS-based device and an optical capture device. For every finger, 12 samples are taken with both sensors from 330 subjects. The resolution of image samples is 300 × 300 and 256 × 400 for sensors 1 and 2, respectively. FVC2006 DB1-A is obtained using an electric Field sensor having an image resolution of 250 dpi. It contains 12 fingerprint samples from 140 subjects. All acquired samples are 256 gray-levels fingerprint images in BMP format. The IITD PolyU iris database contains 5 eye images of both eyes from 224 subjects. The images are captured using a digital CMOS camera of size 320 × 240 pixels. Casia IrisV1 database consists of a total of 756 iris images obtained from 108 subjects. All sample images have a resolution of 320 × 280 and are in BMP format. MMU2 Iris database contains 995 iris images from 100 volunteers having resolution 320 × 238 in BMP format.

The experimental validation is performed on three chimeric datasets namely D1, D2, and D3. D1 contains fingerprint samples of N different subjects from the MCYT database (sensor 1) and IITD iris PolyU database. Thus, a virtual multimodal dataset is created for N subjects by combining the above-mentioned datasets. Similarly, D2 is created by combining N distinct subjects from the MCYT database (sensor 2) and the Casia Iris-V1 database. Also, the D3 dataset is obtained by combining N distinct subjects from the MMU2 iris database and the FVC2006 DB1-A database. Further, all the subjects in D1, D2, and D3 databases are completely different. In addition, fivefold cross-validation is carried out to obtain balanced results. The proposed system

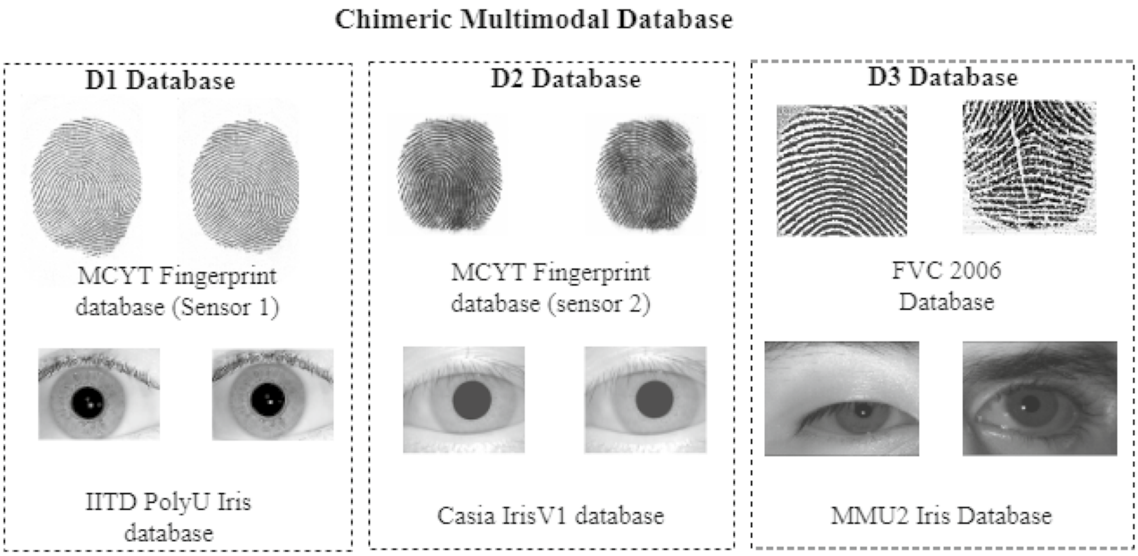


Fig. 3 Sample multimodal database images from the benchmark datasets

is implemented over a hardware configuration of the Intel i3 processor and 4GB RAM using the MATLAB 2018a platform. The performance analysis of the proposed system is discussed in the next section.

4.2 Performance analysis

The proposed system's performance is quantitatively analyzed by means of various performance metrics, namely decidability index (DI), equal error rate (EER), and recognition index (RI). Also, the results thus obtained are compared with other state-of-the-art techniques. During this process, the same techniques for generic feature extraction and score calculation are used for evaluating other methods.

4.2.1 Performance metrics

The difference between the imposter and genuine scores is quantified using decidability index (DI) and is calculated using Eq. 14

$$\mathrm{DI} = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 - \sigma_i^2)/2}} \tag{14}$$

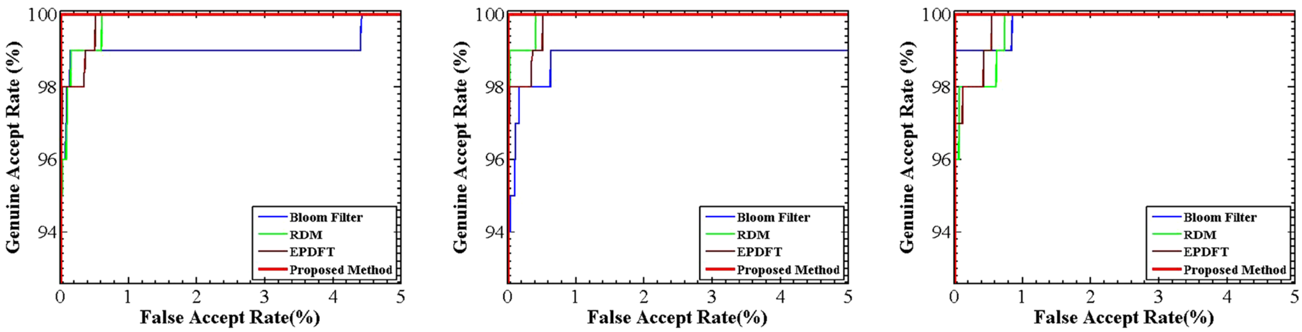
Here, μ_g, μ_i denotes the mean values, and σ_g and σ_i denotes the standard deviation values of score distributions for genuine and imposter, respectively. A high decidability index value suggests a higher ability of the classifier to separate genuine from imposters. Values of decidability index are shown in Table 1 for individual and proposed classifier over chimeric datasets D1, D2, and D3. Equal error rate (EER) is calculated by plotting ROC curves wherein the false acceptance rate (FAR) is plotted against the genuine acceptance rate (GAR). It provides the measure of the accuracy of the proposed biometric system. Recognition index (RI) provides the recognition rate at rank-1 and used for performance evaluation. Cumulative matching characteristics (CMC) curves show the relationship between rank and the recognition rate.

4.2.2 Accuracy analysis

The accuracy of the proposed system is analyzed and compared with state-of-the-art techniques using performance metrics, namely EER, DI, and RI. The performance metric

Table 1 Comparison of EER, DI, and RI values for D1, D2 and D3 databases

Method	DB								
	D1 Database			D2 Database			D3 Database		
	EER	DI	RI	EER	DI	RI	EER	DI	RI
RDM [32]	0.60 ± 0.23	7.28 ± 0.35	97 ± 0.25	0.40 ± 0.19	7.68 ± 0.37	98 ± 0.75	0.71 ± 0.21	7.11 ± 0.19	99 ± 0.50
Bloom filter [36]	0.97 ± 0.20	5.77 ± 0.42	96 ± 0.50	1.14 ± 0.24	4.98 ± 0.28	97 ± 0.45	0.92 ± 0.17	5.33 ± 0.31	98 ± 0.58
EPDFT [50]	0.49 ± 0.32	7.96 ± 0.42	98 ± 1.11	0.78 ± 0.24	6.21 ± 0.46	97 ± 0.90	0.61 ± 0.25	5.79 ± 0.18	97 ± 0.80
Proposed method	0.005 ± 0.004	22.14 ± 0.34	99 ± 0.94	0.003 ± 0.005	18.45 ± 0.43	99 ± 0.95	0.004 ± 0.10	9.71 ± 0.22	99 ± 0.90



(a) D1 Database **(b)** D2 Database **(c)** D3 Database

Fig. 4 Performance comparision of evaluated methods: ROC curves for D1, D2 and D3 database. **a** ROC curves for various cancelable biometric techniques over Database D1. **b** ROC curves for various cancelable biometric techniques over Database D2. **c** ROC curves for various cancelable biometric techniques over Database D3

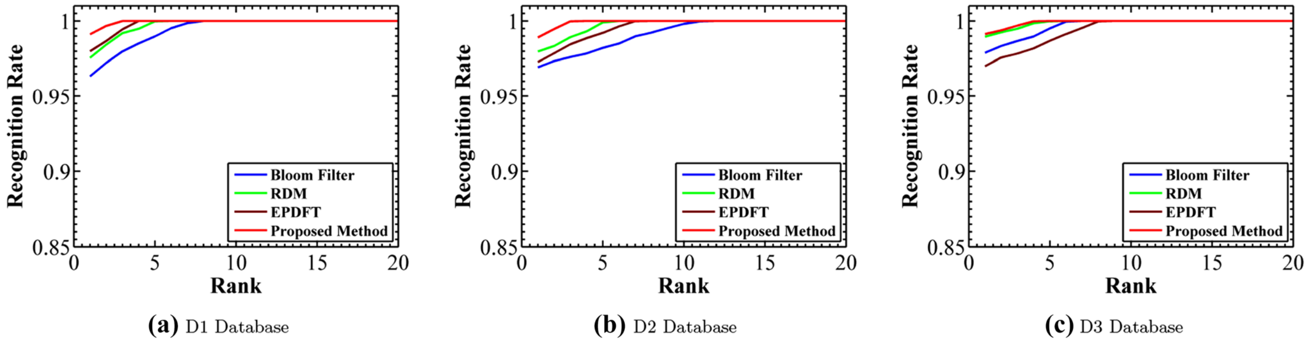


Fig. 5 CMC curves for D1, D2 and D3 databases. **a** Comparison of CMC curves of various cancelable biometric techniques over Database D1. **b** Comparison of CMC curves of various cancelable biometric techniques over Database D2. **c** Comparison of CMC curves of various cancelable biometric techniques over Database D3

values for various methods viz. Random distance method (RDM) [32], bloom filters [36] and enhanced partial discrete Fourier transform (EP-DFT) [50] are compared with the proposed method in Table 1.

The EER value for the proposed score level fusion method is 0.005 for the D1 database, 0.003 for the D2 database and 0.004 for the D3 database which is lowest in comparison with other state-of-the-art methods. The efficiency of the proposed system is also depicted by a high decidability value of 22.14 for the D1 database, 18.45 for the D2 database and 9.71 for the D3 database and supported by ROC and CMC curves in Figs. 4 and 5, respectively. The variation among EER values is due to the use of different datasets and fivefold cross-validation.

Accuracy analysis reveals that the limitations of individual classifiers were effectively addressed by the proposed fusion method providing higher accuracy and more reliable results. The proposed system also improves the privacy of every user making it robust against various issues like template thefts and safeguarding the identity of every user which is also discussed in the next subsection.

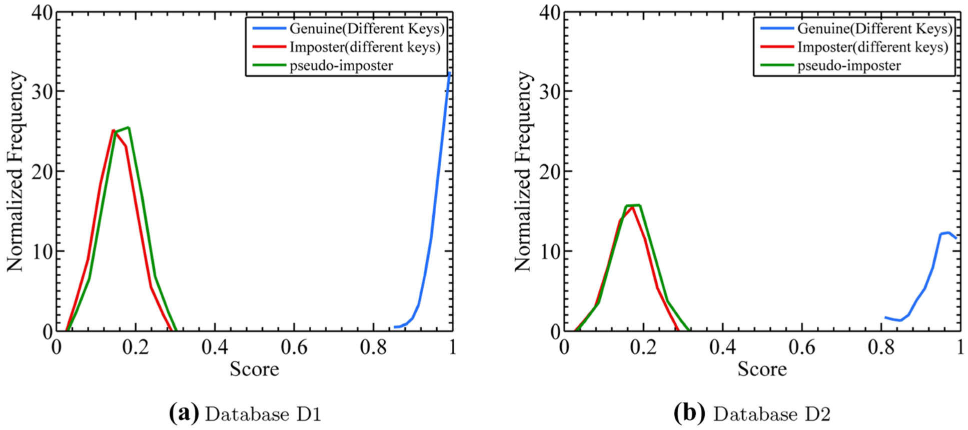
4.3 Privacy analysis

The performance analysis confirms the high accuracy of the proposed system by means of various performance metrics. The proposed biometric system also ensures user privacy by exhibiting the properties like non-invertibility, revocability, and unlinkability.

4.3.1 Non-invertibility

In order to fulfill the criteria of non-invertibility, it must be infeasible to create the original biometric traits even if the key and the transformed template both are compromised. In a situation when both user-specific key and transformed templates are stolen, non-invertibility in the proposed method is achieved by choosing only the azimuth(θ) values during the generation of cancelable templates. Since 67% of the information is discarded, it is not possible to trace back to the original points of projection. Even if points of projection are estimated, it is impossible to find the actual source of projection as there can be infinite points over that line connecting the feature point, Q and projected point on the plane,

Fig. 6 Comparision of genuine, imposter and pseudo-imposter distribution for **a** D1 Database and **b** D2 Database



P. Thus, the proposed method exhibits non-invertibility of biometric templates.

4.3.2 Revocability

For a cancelable biometric system, if the stored templates are stolen, then they are discarded and new templates are generated using a new set of keys. Revocability states that templates generated from the same features should not be correlated. The revocability test is performed to measure the difference between the newly generated template and the old template. In order to check the revocability of the proposed system, 100 different keys were used to obtain 100 transformed templates. Every new user-specific key generates a different random plane and hence different templates. The distribution of imposter vs pseudo-imposter is shown in Fig. 6 which shows that the pseudo-imposter distribution is very similar to imposter distribution. It shows that there is no correlation between the old and new transformed templates. This suggests that transformed templates are treated as different individuals but they were created from the biometric features of the same subject. Thus, the revocability analysis shows that the stolen template can be easily replaced by a new template by using a different set of keys in the proposed system.

4.3.3 Unlinkability

Unlinkability states that multiple biometric templates of a single subject must be unlinkable provided different keys are used. This secures the identity of the subject when it is enrolled in multiple applications. In order to analyze unlinkability, the procedure described in [51] is adopted. For this, pseudo-genuine scores are introduced which refers to the match scores between the different templates of the same user by using different user-specific keys. Also, the pseudo-imposter scores are also calculated between different templates generated using a different user-specific key. In this scenario, if we plot the pseudo-imposter and pseudo-genuine distribution, the overlapping nature of both the distribution suggests that the templates generated from the same or different users are indistinct in nature which is also evident from Fig. 7. On the other hand, if pseudo-genuine and pseudo-imposter distributions are separated, it will be easier to identify the templates from the same user. The struggle in differentiating the templates leads to the unlinkability of the system.

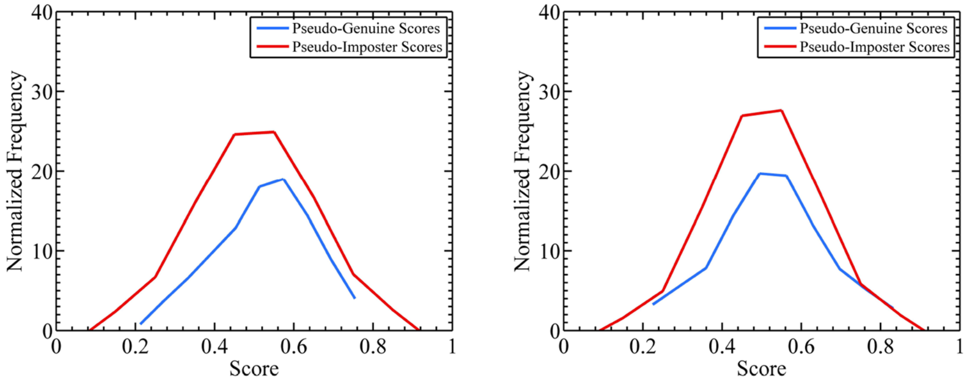
Privacy analysis clearly indicates that the proposed system preserves the privacy of each user by means of revocability, unlinkability, and non-invertibility. The complementary traits are fused together generating a cancelable template making system highly secure and robust against various attacks which are discussed in the next subsection.

4.4 Security analysis

The security of the biometric system is of utmost priority. No adversary, in any case, may be able to break through the system as it will arise many security problems. The proposed biometric system is also analyzed against many such attacks.

4.4.1 Brute force attack

Brute Force attack assumes that the adversary possesses no previous knowledge about the transformed or the original biometric feature. Each possible combination is used to generate and match a transformed template. In the worst-case scenario, let us assume the intruder knows the length of the template and the maximum value and the minimum value of the transformed template. In the proposed approach, the maximum and minimum values of template elements are -3.14165834 and 3.14165834 in DB1 with a precision of each element set to 8 decimal digits which amount to a total



(a) Database D1

(b) Database D2

Fig. 7 Comparision of pseudo-genuine and pseudo-imposter distribution for **a** D1 Database and **b** D2 Database

of 2^{29} possibilities for each element in the template. Hence, to generate a template it would require an exceptionally high brute force effort which makes it computationally infeasible.

4.4.2 Attacks via record multiplicity

During attacks via record multiplicity (ARM), the adversary possesses multiple transformed templates of the same user and tries to establish a connection so as to develop an image of the original biometric trait. For example, let us take two transformed templates T1 and T2 created using a different key for the same user. Also, during privacy analysis, unlinkability between these templates was proven experimentally. Further, the ith value of T1 depends upon the point of projection P_1 and it cannot be connected to ith value of T2 as it depends upon its points of projection $P_2.P_1$ and P_2 will always be different as different keys are chosen. Therefore, the attacker cannot mount ARM attack even after having different copies of transformed templates from the same user.

4.4.3 Blended substitution attacks

In the blended substitution, the attacker combines its data with user data in a single template. The blended template allows both users and attackers to authenticate against the same ID simultaneously. In the proposed approach, blended substitution is not feasible since, with only half of the user or attacker's attribute, the matching score would be rejected as an imposter for both user and attacker.

In sum, the proposed system is an accurate, highly robust and reliable solution that can be employed in critical applications. The generated cancelable templates are highly non-invertible, unlinkable and revocable and hence address privacy and security concerns.

5 Conclusion and future directions

In this paper, a multimodal biometric system is proposed that ensures not only high performance but also robustness to security and privacy concerns. The feature size is reduced to half thereby requiring low computational and space complexity. The security analysis of the proposed fusion mechanism shows that the approach is able to defend various attacks, thereby, assuring user-privacy and data-security. Moreover, the generated templates are highly revocable, thus can be regenerated in case the data gets compromised. Hence, the proposed approach can be deployed for biometric authentication in security-critical applications. Experimental analysis shows the effectiveness of the proposed method in comparison to state-of-the-art solutions. On average, the proposed fusion achieves DI of 16.63 and EER of 0.004.

In future, we will look forward to incorporate image quality as a reliability factor into the proposed cancelable biometric system. It will help in enhancing the adaptivity of the system so that it may address various other challenges like poor quality input images, improper sensor interaction, etc. The reliability factor can be learned over a time period by estimating image quality for specific users and can make the system highly reliable and robust. The work can also be extended to integrate different security levels in the proposed framework.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Gupta, K., Walia, G.S., Sharma, K.: Quality based adaptive score fusion approach for multimodal biometric system. Appl. Intell. **50**, 2824–2836 (2019)
2. Ross, A., Jain, A.: Information fusion in biometrics. Pattern Recogn. Lett. **24**(13), 2115–2125 (2003)
3. Gupta, K., Walia, G.S., Sharma, K.: Multimodal Biometric System using Grasshopper Optimization. In: 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 387–391. IEEE (2019)
4. Ross, A., Jain, A.K.: Multimodal biometrics: an overview. In: 12th European Signal Processing Conference, 1221–1224. IEEE (2004)
5. Haghighat, M., Abdel-Mottaleb, M., Alhalabi, W.: Discriminant correlation analysis: real-time feature level fusion for multimodal biometric recognition. IEEE Trans. Inf. Forensics Secur. **11**(9), 1984–1996 (2016)
6. 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)
7. Pillai, J.K., Patel, V.M., Chellappa, R., Ratha, N.K.: Sectored random projections for cancelable iris biometrics. In: IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1838–1841 (2010)
8. Pillai, J.K., Patel, V.M., Chellappa, R., Ratha, N.K.: Secure and robust iris recognition using random projections and sparse representations. IEEE Trans. Pattern Anal. Mach. Intell. **33**(9), 1877–1893 (2011)
9. Savvides, M., Kumar, B.V., Khosla, P.K.: Cancelable biometric filters for face recognition. In: Proceedings of the 17th International Conference on Pattern Recognition. ICPR 2004, vol. 3, pp. 922–925. IEEE (2004)
10. Maiorana, E., Campisi, P., Fierrez, J., Ortega-Garcia, J., Neri, A.: Cancelable templates for sequence-based biometrics with application to on-line signature recognition. IEEE Trans. Syst. Man Cybern. Part A Syst. Hum. **40**(3), 525–538 (2010)
11. Jin, A.T.B., Ling, D.N.C., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn. **37**(11), 2245–2255 (2004)
12. Zuo, J., Ratha, N.K., Connell, J.H.: Cancelable iris biometric. In: 2008 19th International Conference on Pattern Recognition, pp. 1–4. IEEE (2008)

13. Nandakumar, K., Jain, A.K.: Biometric template protection: bridging the performance gap between theory and practice. IEEE Signal Process. Mag. **32**(5), 88–100 (2015)
14. Patel, V.M., Ratha, N.K., Chellappa, R.: Cancelable biometrics: a review. IEEE Signal Process. Mag. **32**(5), 54–65 (2015)
15. Teoh, A.B.J., Yip, W.K., Toh, K.-A.: Cancellable biometrics and user-dependent multi-state discretization in BioHash. Pattern Anal. Appl. **13**(3), 301–307 (2010)
16. Teoh, A.B., Goh, A., Ngo, D.C.: Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Trans. Pattern Anal. Mach. Intell. **28**(12), 1892–1901 (2006)
17. Teoh, A.B.J., Yuang, C.T.: Cancelable biometrics realization with multispace random projections. IEEE Trans. Syst. Man Cybern. Part B (Cybernetics) **37**(5), 1096–1106 (2007)
18. Wang, Y., Plataniotis, K.N.: An analysis of random projection for changeable and privacy-preserving biometric verification. IEEE Trans. Syst. Man Cybern. Part B (Cybernetics) **40**(5), 1280–1293 (2010)
19. Paul, P.P., Gavrilova, M., Klimenko, S.: Situation awareness of cancelable biometric system. Vis. Comput. **30**(9), 1059–1067 (2014)
20. Yang, B., Hartung, D., Simoens, K., Busch, C.: Dynamic random projection for biometric template protection. In: 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1–7. IEEE (2010)
21. Lacharme, P., Cherrier, E., Rosenberger, C.: Preimage attack on biohashing. In: 2013 International Conference on Security and Cryptography (SECRYPT), pp. 1–8. IEEE (2013)
22. Sadhya, D., Raman, B.: Generation of cancelable Iris templates via randomized bit sampling. IEEE Trans. Inf. Forensics Secur. **14**(11), 2972–2986 (2019)
23. Wang, S., Hu, J.: Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recogn. **47**(3), 1321–1329 (2014)
24. Sharma, R.P., Dey, S.: Fingerprint liveness detection using local quality features. Vis. Comput. **35**(10), 1393–1410 (2019)
25. Ali, S.S., Ganapathi, I.I., Prakash, S., Consul, P., Mahyo, S.: Securing biometric user template using modified minutiae attributes. Pattern Recogn. Lett. **129**, 263–270 (2020)
26. Trivedi, A.K., Thounaojam, D.M., Pal, S.: Non-Invertible cancellable fingerprint template for fingerprint biometric. Comput. Secur. (2020). https://doi.org/10.1016/j.cose.2019.101690
27. Wu, S.-C., Chen, P.-T., Swindlehurst, A.L., Hung, P.-L.: Cancelable biometric recognition with ECGs: subspace-based approaches. IEEE Trans. Inf. Forensics Secur. **14**(5), 1323–1336 (2019)
28. Rathgeb, C., Busch, C.: Cancelable multi-biometrics: mixing iris-codes based on adaptive bloom filters. Comput. Secur. **42**, 1–12 (2014)
29. Kumar, N., Singh, S., Kumar, A.: Random permutation principal component analysis for cancelable biometric recognition. Appl. Intell. **48**(9), 2824–2836 (2018)
30. Dwivedi, R., Dey, S.: A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. Appl. Intell. **49**(3), 1016–1035 (2019)
31. Walia, G.S., Rishi, S., Asthana, R., Kumar, A., Gupta, A.: Secure multimodal biometric system based on diffused graphs and optimal score fusion. IET Biom. **8**(4), 231–242 (2019)
32. Kaur, H., Khanna, P.: Random distance method for generating unimodal and multimodal cancelable biometric features. IEEE Trans. Inf. Forensics Secur. **14**(3), 709–719 (2018)
33. Walia, G.S., Jain, G., Bansal, N., Singh, K.: Adaptive weighted graph approach to generate multimodal cancelable biometric templates. IEEE Tran. Inf. Forensics Secur. (2019). https://doi.org/10.1109/TIFS.2019.2954779
34. Paul, P.P., Gavrilova, M.L.: A novel cross folding algorithm for multimodal cancelable biometrics. Int. J. Softw. Sci. Comput. Intell. **4**(3), 20–37 (2012)
35. Chin, Y.J., Ong, T.S., Teoh, A.B.J., Goh, K.: Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Inf. Fusion **18**, 161–174 (2014)
36. Gomez-Barrero, M., Rathgeb, C., Li, G., Ramachandra, R., Galbally, J., Busch, C.: Multi-biometric template protection based on bloom filters. Inf. Fusion **42**, 37–50 (2018)
37. Abdellatef, E., Ismail, N.A., Elrahman, S.E.S.A., Ismail, K.N., Rihan, M., El-Samie, F.E.A.: Cancelable multi-biometric recognition system based on deep learning. Vis. Comput. **2**, 1–13 (2019)
38. Das, R., Piciucco, E., Maiorana, E., Campisi, P.: Convolutional neural network for finger-vein-based biometric identification. IEEE Trans. Inf. Forensics Secur. **14**(2), 360–373 (2018)
39. Kacar, U., Kirci, M.: ScoreNet: deep cascade score level fusion for unconstrained ear recognition. IET Biom. **8**(2), 109–120 (2019)
40. Liu, L., Ouyang, W., Wang, X., Fieguth, P., Chen, J., Liu, X., Pietikäinen, M.: Deep learning for generic object detection: a survey. Int. J. Comput. Vis. **128**, 1–58 (2019)
41. Ojala, T., Pietikäinen, M., Harwood, D.: A comparative study of texture measures with classification based on featured distributions. Pattern Recogn. **29**(1), 51–59 (1996)
42. Daugman, J.G.: High confidence visual recognition of persons by a test of statistical independence. IEEE Trans. Pattern Anal. Mach. Intell. **15**(11), 1148–1161 (1993)
43. Farina, A., Kovacs-Vajna, Z.M., Leone, A.: Fingerprint minutiae extraction from skeletonized binary images. Pattern Recogn. **32**(5), 877–889 (1999)
44. Sudiro, S.A., Paindavoine, M., Kusuma, T.M.: Simple fingerprint minutiae extraction algorithm using crossing number on valley structure. In: IEEE Workshop on Automatic Identification Advanced Technologies, pp. 41–44 (2007)
45. Daugman, J.: How iris recognition works. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 21–30 (2004)
46. Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V., Satue, A., Hernaez, I., Igarza, J.-J., Vivaracho, C., Escudero, D., Moro, Q.-I.: MCYT baseline corpus: a bimodal biometric database. IEE Proc. Vis. Image Signal Process. **150**(6), 395–401 (2003)
47. Kumar, A., Passi, A.: Comparison and combination of iris matchers for reliable personal authentication. Pattern Recogn. **43**(3), 1016–1026 (2010)
48. Cappelli, R., Ferrara, M., Franco, A., Maltoni, D.: Fingerprint verification competition 2006. Biom. Technol. Today **15**, 7–9 (2007)
49. MMU2 Iris Image Databases. http://pesona.mmu.edu.my/ccteo/. Accessed June 2019 (2008)
50. Yang, W., Wang, S., Hu, J., Zheng, G., Valli, C.: A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recogn. **78**, 242–251 (2018)
51. Jin, Z., Hwang, J.Y., Lai, Y.-L., Kim, S., Teoh, A.B.J.: Ranking-based locality sensitive hashing-enabled cancelable biometrics: index-of-max hashing. IEEE Trans. Inf. Forensics Secur. **13**(2), 393–407 (2017)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Keshav Gupta is currently pursuing his Ph.D. degree in the Computer Science and Engineering Department, Delhi Technological University, New Delhi, India. He completed his M. Tech. in software engineering from Delhi Technological University, New Delhi. His current research interests include biometric systems, pattern recognition, image processing and machine learning. He has published many research papers in reputed international journals and conferences.

Dr. Gurjit Singh Walia received his Ph.D. degree in the field of computer vision from Delhi Technological University (Formerly Delhi College of Engineering), New Delhi, and the M.E. degree in electronics from Punjab Engineering College, Chandigarh. He is working as a Senior Scientist with Defence Research and Development Organization, New Delhi. His current research interests include machine learning, pattern recognition, and information security. He has published over 30 research papers in international journals and conferences. He is Fellow of IETE, Fellow of Institute of Engineering, Senior Member of IEEE, Member of CSI and CRSI. He is reviewer of various IEEE transactions, Elsevier and Springer journals.

Dr. Kapil Sharma is working as a Professor and the Head of Department of Information Technology, Delhi Technological University, Delhi. He has completed Ph.D. Degree in Computer Science from M.D. University, India. He has obtained his B.E. and M.Tech. degrees in Computer Science from M.D. University and IASE, India, respectively. His research interests include system design, pattern recognition, computer vision and soft computing. He has published more than 100 research papers in refereed journals.