RESEARCH ARTICLE

Asian Research Association

INTERNATIONAL RESEARCH JOURNAL OF
MULTIDISCIPLINARY TECHNOVATION

DOI: 10.54392/irjmt2512

Cancelable Biometric Template Generation using Eigenfeature Regularization

Onkar Singh [a, d], Ajay Jaiswal [b, *], Nitin Kumar [c], Naveen Kumar [d]

[a] Shaheed Sukhdev College of Business Studies, University of Delhi, Delhi-110089, India.
[b] School of Open Learning, University of Delhi, Delhi-110007, India.
[c] Department of Computer Science and Engineering, Punjab Engineering College, Chandigarh-160012, India.
[d] Department of Computer Science, University of Delhi, Delhi-110007, India
* Corresponding Author Email: ajayjaiswal@col.du.ac.in

DOI: https://doi.org/10.54392/irjmt2512
Received: 08-10-2024; Revised: 14-12-2024; Accepted: 20-12-2024; Published: 30-12-2024

Abstract: Cancelable biometrics addresses biometric data’s privacy and security concerns. We present two new cancelable biometrics template generation methods: RP-RegSt and RP-RegSb. The suggested approaches use random permutations and regularized eigenfeature extraction to generate cancelable biometrics templates, which can be reissued if compromised. We also show that applying random permutation to generate cancelable biometric templates enhances recognition accuracy. The suggested approaches are tested on six publicly accessible databases: three iris databases (UBIRIS.v1, CASIA-V1, and IITD Iris), two face databases (Georgia Tech and AT&T), and one ear database (IITD Ear). The superiority of the proposed methods is demonstrated by comparing them to three state-of-the-art random permutation-based cancelable biometric template generation techniques. The suggested approaches’ performance on challenging databases with substantial biometric image variation, such as Georgia Tech and UBIRIS, shows their robustness and efficacy. The privacy concern is addressed as the templates are irreversible (non-invertible) and immune to imposter attacks, while brute force analysis shows the templates are secure. The templates satisfy the diversity (unlinkability) and revocability properties.

Keywords: Random Permutation, Cancelable Biometrics, Template Protection, Non-invertible Transformation

1. Introduction

Use of biometrics in user authentication effectively addresses the issue of distinguishing between authorized and unauthorized users having stolen/shared passwords, tokens, etc. This is due to the inherent nature of biometric characteristics, such as fingerprints [1] or facial features [2], which are unique to each individual and cannot be shared or replicated. However, the uniqueness and permanent association of biometric information with a person presents significant concerns about the privacy and security [3]. The intruder can get easy access to the user’s biometric information. For example, fingerprints can be traced from a user’s drinking glass, and the face or iris can be stolen from images from social media or other uploads. Biometric cryptosystems provide security for biometric data through encryption and decryption techniques. These techniques require data decryption for matching and do not allow for matching query images in the encrypted domain [4]. To alleviate these problems, the concept of cancelable biometrics (CB) has been introduced [5]. “It consists of an intentional, repeatable distortion of the biometric signal based on a chosen transform.” In the context of cancelable biometrics (CB), the biometric data undergoes a conversion process in a different domain through a non-invertible transformation. This transformation ensures that the information in the converted domain does not disclose any significant details about the original biometric data. Furthermore, performing matching operations on query images within the transformed domain remains feasible.

There are four fundamental characteristics of the cancelable biometric template [6, 7]:

- *Non-invertibility*: Transformation should be non-invertible to safeguard biometric data.
- *Renewability/Cancelability*: The old template should be canceled, and the new template should be renewed in case of compromise.
- *Diversity/Unlinkability*: Templates corresponding to the same biometrics should not correlate in different applications.
- *Performance*: The conversion of biometric data to a cancelable template should preserve

discriminatory information so that it does not lead to deterioration in recognition performance.

The fundamental characteristic of non-invertibility can be attained by two methods: non-invertible transform approaches and biometric salting [8]. It is important to note that the former approach involves applying a noninvertible transformation to the biometric data to generate a template that cannot be inverted. Furthermore, the second approach transforms the original biometric data into a cancelable template by adding random noises or patterns (person-specific), which may increase the discriminating power of the biometric data and protect the template from potential misuse [4]. However, biometric salting transformations are invertible [9]. The application of cancelable biometric schemes is not only limited to user authentication but includes non-invertible key creation that can be transferred on an unsecured network [10], safeguarding sensitive data of patients, surveillance, corpse identification, etc.

One of the main problems in dealing with biometric images is the high dimensionality, as we consider each pixel's intensity value as a separate feature. For example, a simple grayscale image with a resolution of 500 × 500 has 250,000 features. Working with such high dimensions leads to the problem of the *curse of dimensionality* [11]. Some major disadvantages of working in such high dimensionality include a) overfitting of the training data, b) high computational complexity, and c) making it challenging to find the pattern. The curse of dimensionality is often referred to as the *small sample size* (SSS) problem because the number of samples (total number of images in our case) is much lower than the number of features (number of pixels in the image) per sample [12]. Many techniques are given in the literature to deal with this problem such as Principal Component Analysis (PCA) [13, 14], Bayesian Maximum Likelihood (BML) [15], Independent Component Analysis (ICA) [16, 17], Locality Preserving Projection (LPP) [18], and Linear Discriminant Analysis (LDA) [19]. These techniques are not only used for dimensionality reduction but are also used for face recognition. PCA and LDA are the most popular. PCA aims to find the dimensions where the variance is captured maximum, while LDA seeks to find the directions where maximum separability is captured. It has been proven that Fisher's LDA is better than PCA for class separability [14]. To maximize the separability, LDA aims to minimize the within-class scatter while maximizing the between-class scatter. It uses the inverse of the within-class matrix for this, but because of SSS problem, it often results in a singular within-class matrix [20].

1.1 Motivation and Research Gaps

The PCA, LPP, and LDA were successfully used in cancelable biometrics to transform the biometric images into cancelable templates. For example, random permutation principal component analysis (RP-PCA) and random permutation two-dimensional principal component analysis (RP-2DPCA) use PCA and 2DPCA [3], random permutation-based linear discriminant analysis (RPLDA) uses LDA [21], and random permutation-based locality preserving projection (RP-LPP) uses locality preserving projection [22]. All of these cancelable biometric template generation methods solve the problem of the curse of dimensionality (also known as SSS) by reducing the dimension using the techniques as mentioned above. The singular within-class matrix issue is not addressed while applying LDA for the cancelable biometrics in [21]. The issue of the singularity in the within class matrix is addressed in face recognition in Fisher's LDA (FLDA) [14], Direct LDA (DLDA) [23], the Null space method or NLDA [24], etc. However, these techniques either ignore the null subspace or focus only on the null subspace. Eigenfeature regularization and Extraction (ERE) [25] is proposed for face recognition and decomposes the eigenspace of the within-class matrix into three subspaces: face, noise, and null subspace. The proposed work solves the issue of a singular within-class matrix of LDA in cancelable biometrics using ERE and tries to answer the following research questions:

- Is it feasible to use the concept of eigenfeature regularization and extraction in cancelable biometrics?
- Does the application of eigenfeature regularization in cancelable biometrics work for biometric traits other than the face, like an iris or an ear?
- How does applying random permutation with eigenfeature regularization affect the recognition accuracy?

1.2 Contribution

This paper suggests two novel cancelable biometric template generation methods based on random permutation and regularized eigenfeatures. The methods are two-factor authentication methods, where the person must enter the correct key/Personal Identification Number (PIN) along with the presented biometrics. We have made the following contributions to the field of cancelable biometrics as a result of our research efforts:

- Two new cancelable biometrics approaches to generate the cancelable biometric templates using random permutation with eigenfeature regularization and extraction.
- We have shown that the random permutation improves classification accuracy apart from offering cancelability.

- The proposed methods are not modality-specific rather can be used for other modalities.
- The proposed approaches surpass the recognition performance of the other baseline approaches that generate cancelable biometric templates based on random permutation.

The rest of the paper is divided into five more sections. The literature related to the proposed methods is discussed in Section 2, where subsection 2.1 discusses using a random permutation to generate cancelable biometric templates. Section 2.2 discusses regularizing eigenfeatures, feature extraction, and dimensionality reduction. Section 3 presents the proposed method, which uses eigenfeature regularization with random permutation for cancelable biometrics template generation in detail. The experimental setup is described in Section 4, which gives the complete details of biometric image databases used to assess the proposed method. Section 5 analyses the experiments' results, where the proposed methods are compared with other random permutation-based methods to generate the cancelable template. In section 6, we give the proposed work's conclusions and future research directions.

2. Related Work

The literature uses various approaches for template generation. The cancelable biometric approaches can be classified into ten distinct types [26] (i) Non-invertible Geometric Transforms, (ii) Random Projections, (iii) Cancelable Biometric Filters, (iv) Bioconvolving, (v) Bloom Filters, (vi) Knowledge Signatures, (vii) Biohashing Methods, (viii) Random Permutations, (ix) Salting Methods, and (x) Hybrid Methods. Preserving discriminating information in the resulting template is difficult in most categories, except random permutation-based approaches [22].

2.1 Random Permutation in Cancelable Biometrics

The application of random permutation in cancelable biometrics was first introduced in two techniques, i.e. GRAY-COMBO and BIN-COMBO [27]. The method GRAY-COMBO is used to generate a cancelable template for grayscale iris images, whereas the BIN-COMBO is used for binary images. In the first method, GRAYCOMBO, the rows are shifted circularly in the horizontal direction using the random offset. Then, the randomly selected rows are combined using the addition or multiplication operation. The random offset and random selection of rows are person-specific. In BIN-COMBO, the template is generated similarly to the first method, except that the XOR/XNOR operation combines the randomly selected rows in place of addition/multiplication.

The random permutation is also used in RPPCA [3], RP-2DPCA [3], RP-LPP [22], and RPLDA [21]. The cryptic pattern is generated first using a random permutation matrix, and features are then extracted to reduce the dimensions and make the template non-invertible using PCA, LPP, and LDA in RP-PCA, RP-LPP, and RPLDA, respectively. In another approach called random permutation max out (RPM) [28], RPM transforms a continuous face feature vector into a max-ranked indices vector as a cancelable template using a person-specific stacked permutation array. In a different approach, the fingerprint vectors are first converted into a binary string and then randomly permuted to generate the cancelable fingerprint template [1]. In recent work, the random permutation-based linear regression for cancelable biometrics (RP-LRCB) [29] first generates a virtual image using linear regression. Then, a cancelable template is generated using random permutation from the virtual image.

2.2 Eigenfeature Regularization and Features Extraction

In this section, the process of eigenfeature regularization is discussed in detail. The algorithm of eigenfeature regularization and extraction (ERE) is given in [25]. It mainly consists of the following six steps:

1. Computing within-class matrix from the training data.
2. Extraction of eigenfeatures.
3. Regularization of eigenvalues.
4. Transforming the training set.
5. Extracting the eigenvectors from transformed data.
6. Dimension reduction and feature extraction.

Let the training set contain N different classes, where each class represents a person and each having m biometric images of size $w \times h$. The training set's total number of images is $n = N \times m$. The column vector x_{ij} is used to represent the j^{th}biometric image of i^{th} person and $x_{ij} \in \mathbb{R}^{q=w\times h}$.

2.2.1 Computing within-class matrix

The within class matrix minimizes the intra-class variance in the linear discriminant analysis. Assuming all classes have equal prior probability i.e. $p_i = \frac{1}{N}$, then the within-class scatter matrix, S_w, is defined as [25]:

$$\mathrm{S}_w = \sum_{i=1}^{N} \frac{p_i}{m} \sum_{j=1}^{m} \left(x_{ij} - \bar{x}_i\right) \left(x_{ij} - \bar{x}_i\right)^T \quad (1)$$

where $\bar{x}_i = \frac{1}{m}\sum_{j=1}^{m} x_{ij}$ represents the mean image of each class.

2.2.2 Extraction of eigenfeatures

The eigendecomposition of S$_w$ is used to obtain the diagonal matrix Λ containing eigenvalues $[\lambda_1, \lambda_2, \ldots, \lambda_q]$ and the matrix Θ containing eigenvectors $[\theta_1 \theta_2 \ldots \theta_q]$. The $\Lambda$and the associated Θ are sorted in the decreasing order of eigenvalues.

2.2.3 Regularization of eigenvalues

The eigenspace of S$_w$ is then decomposed into face subspace ($\mathrm{F} = \{\theta_k\}_{k=0}^{m}$), noise subspace ($\mathrm{N} = \{\theta_k\}_{k=m+1}^{r}$), and null subspace ($\emptyset = \{\theta_k\}_{k=r+1}^{q}$). The r is the rank of the matrix, forS_t, $r \leq min(q, n-1)$, for S_b, $r \leq min(q, N-1)$, and for S_w, $r \leq min(q, n-N)$. The S_t and S_b are the total scatter and between-class scatter matrices. The noise subspace starts with $m + 1^{th}$ eigenvalue of the within-class scatter matrix, which can be calculated as :

$$\lambda_{m+1}^{w} = max\{\forall \lambda_k^w | \lambda_k^w < \left(\lambda_{med}^{w} + \mu(\lambda_{med}^{w} - \lambda_r^w)\right)\} \quad (2)$$

where λ_{med}^{w} is the median eigenvalue of the face & noise subspace and calculated as $\lambda_{med}^{w} = median\{\lambda_k^w | k \leq r\}$. The μ is the constant and is taken as 1. The variation of the face component in the face subspace is high, in the noise subspace it is very low, and almost zero in the null space. Therefore, the weights with the face structural components are added to the noise and null subspace. The two constants α and β for the eigenvalue regularization are computed as follows:

$$\alpha = \frac{\lambda_1^w \lambda_m^w (m-1)}{\lambda_1^w - \lambda_m^w}, \beta = \frac{m\lambda_m^w - \lambda_1^w}{\lambda_1^w - \lambda_m^w} \quad (3)$$

The eigenvalues of the within-class matrix S$_w$ can be regularized using the constants α and β obtained in equation (3) in the following manner [25]:

$$\tilde{\lambda}_k^w = \begin{cases} \lambda_k^w, k < m \\ \frac{\alpha}{k+\beta}, m \leq k \leq r \\ \frac{\alpha}{r+1+\beta}, r < k \leq q \end{cases} \quad (4)$$

2.2.4 Transforming the training set

After regularizing the eigenvalues, the corresponding weights are computed as follows [25]:

$$w_k^w = \frac{1}{\sqrt{\tilde{\lambda}_k^w}} k = 1, \ldots, q \quad (5)$$

The weighted eigenvectors are now used to transform the training set X as:

$$Y = \tilde{\Theta}_w^T X \quad (6)$$

where the weighted eigenvectors are $\tilde{\Theta}_w =$

$[w_k^w \theta_k^w]_{k=1}^{q} = \{w_1^w \theta_1^w, w_2^w \theta_2^w, \ldots, w_q^w \theta_q^w\}$and X is the training set.

2.2.5 Extracting the eigenvectors from transformed data

Now, the transformed training set Y containing regularized eigenfeatures is used to extract the features using the total scatter matrix and between-class scatter matrix as follows:

$$\tilde{S}_t = \sum_{i=1}^{N} \frac{p_i}{m} \sum_{j=1}^{m} \left(y_{ij} - \overline{y}_i\right) \left(y_{ij} - \overline{y}_i\right)^T \quad (7)$$

$$\tilde{S}_b = \sum_{i=1}^{N} p_i \, (\overline{y}_i - \overline{y})(\overline{y}_i - \overline{y})^T \quad (8)$$

where $y_{ij} \in \mathbb{R}^q$ is a vector of Y, $\bar{y} = \frac{1}{N} \Sigma_{i=1}^{N} \bar{y}_i$, and $\bar{y}_i = \frac{1}{m} \Sigma_{j=1}^{m} y_{ij}$.

2.2.5 Dimension reduction and feature extraction

The eigendecomposition is then applied to the between-class scatter matrix $\tilde{S}_b$ and the total scatter matrix $\tilde{S}_t$ to get the eigenvectors Θ_b and Θ_t. After sorting the eigenvectors in the decreasing order of their associated eigenvalues, the first d eigenvectors from $\tilde{S}_b$or $\tilde{S}_t$ are used to reduce the dimension where $d <<$ q. The reduced sets of eigenvectors are $\tilde{\Theta}_b \in \mathbb{R}^{q \times d}$and $\tilde{\Theta}_t \in \mathbb{R}^{q \times d}$. The feature regularization and extraction matrix for the between-class scatter matrix is constructed as follows [25]:

$$U_b = \tilde{\Theta}_w \tilde{\Theta}_b \quad (9)$$

The matrix $U_b \in \mathbb{R}^{q \times d}$is used to extract features from the original training set as:

$$F = U_b^T X \quad (10)$$

A similar feature regularization and extraction matrix $U_t \in \mathbb{R}^{q \times d}$ can be constructed using the eigenvectors $\tilde{\Theta}_t$ of the total scatter matrix, and the reduced features set can be extracted from the training set.

3. The Proposed Approach

The approaches such as RP-PCA [3], RPLDA [21], and RP-LPP [22] are suggested in the literature to generate the cancelable templates while simultaneously reducing the dimension. LDA outperforms PCA for large datasets [30]. But, because of the small sample size (SSS) and high dimensionality, the singular matrix problem arises in LDA [12]. The eigenfeature regularization and extraction (ERE) [25] is suggested to solve the singular matrix problem. In this section, we propose two methods to generate cancelable biometric templates for grayscale images using random permutation and eigenfeature regularization and extraction (ERE), which we will call *RP-RegSt* and *RP-RegSb*.

3.1 Random Permuted-based Eigenfeatures Regularization

The process of cancelable template generation comprises two phases. In the first phase, we construct a cryptic pattern set and transform it using regularized eigenfeatures. In the second phase, we generate the templates from the transformed cryptic pattern set. The complete process is described in Algorithm 1.

Each person in the database represents a class. Suppose we have N different classes in the training set, and a set of m images represents each class. All the images in the database have the same resolution: $a \times b$ where a and b denote the width and height of the image, respectively.

```
Algorithm 1: Cancelable Template Generation
Input: Training set $X$ and set of keys $K$
Output: Cancelable template set $T$
1  For each person, compute a personalized Random Permutation Matrix $P_i$ using person-specific key $k_i$
2  Compute the set of cryptic patterns $Z$ from the training set $X$ using $P$
3  Compute the within-class matrix $S'_w$ for the cryptic patterns set $Z$
4  Regularize the eigenfeatures of $S'_w$ using ERE
5  Transform $Z$ using regularized eigenfeatures
6  Generate template set $T$ using either between class scatter matrix or total scatter matrix
```

Let j^{th} biometric image of i^{th} person/class be represented using a matrix $u_{ij} \in \mathbb{R}^{a \times b}$. The two-dimensional images in the database are transformed into column vectors. Thus, $u_{ij} \in \mathbb{R}^{a \times b} \mapsto x_{ij} \in \mathbb{R}^{q \times 1}$, where $q = a \times b$.

As the training set comprises m images for each of the N classes, we have a total of $n = N \times m$ images. Thus, the training set X is defined as a matrix in the following way:

$$X = [x_{11}x_{12} \dots x_{N(m-1)}x_{Nm}] \in \mathbb{R}^{q \times n} \tag{11}$$

and class is defined through a matrix. For example, i^{th}class is represented as follows:

$$X_i = [x_{i1}x_{i2} \dots x_{im}] \in \mathbb{R}^{q \times m} \quad i = 1, \dots, N \tag{12}$$

For i^{th} class, a unique Boolean random permutation matrix $P_i \in \mathbb{B}^{q \times q}$ is generated using their personalized key as the seed. The random permutation matrix is generated by permuting rows of the identity matrix. The permuted biometric image z_{ij} (also known as a cryptic pattern) for x_{ij} is obtained as follows:

$$z_{ij} = P_i x_{ij} \tag{13}$$

Thus, the matrix Z_i corresponding to class X_i is computed as the dot product of P_i and X_i:

$$Z_i = P_i \cdot X_i \tag{14}$$

The cryptic pattern matrix corresponding to the full training set now becomes:

$$Z = [z_{11}z_{12} \dots z_{N(m-1)}z_{Nm}] \in \mathbb{R}^{q \times n} \tag{15}$$

The within-class matrix S'_w for the matrix of cryptic patterns is computed as follows:

$$S'_w = \sum_{i=1}^{N} \frac{1}{n} \sum_{j=1}^{m} (z_{ij} - \overline{z_i})(z_{ij} - \overline{z_i})^T \tag{16}$$

where $\bar{z}_i = \frac{1}{m} \sum_{j=1}^{m} z_{ij}$. Next, we apply the eigendecomposition on S'_w to extract the eigenfeatures as follows:

$$\Lambda = \Omega^{-1} S'_w \Omega \tag{17}$$

where Λ is a diagonal matrix of eigenvalues, say, $\lambda_1, \lambda_2, \dots, \lambda_q$, and Ω is the matrix of eigenvectors $(\omega_1\omega_2 \dots \omega_q)$. The Λ and the associated vectors in Ω are sorted in the decreasing order of eigenvalues. Following [25], the eigenvalues of S'_w are regularized using equations (2), (3), and (4), and the weights $[w_j]_{j=1}^{q}$ are calculated using equation (5) to find the weighted eigenvectors $\tilde{\Omega}_w$. The matrix Z containing the cryptic patterns of all the classes is transformed as:

$$V = \tilde{\Omega}_w^T Z \tag{18}$$

where the weighted eigenvectors are $\tilde{\Omega}_w = [w_i\omega_i]_{i=1}^{q} = \{w_1\omega_1, w_2\omega_2, \dots, w_q\omega_q\}$ and $[w_j]_{j=1}^{q}$ are weights computed using equation (5).

3.2 Template Generation

Random permutation enhances the security and privacy of biometric information while maintaining low computing complexity [4]. The proposed template generation method employs random permutation through personalized keys to generate cancelable templates. If compromised, changing the personalized key can produce a new template; hence, using personalized keys to generate the template is advantageous. The changed key results in a fresh permutation matrix, generating a novel cancelable template uncorrelated with the stolen one [31, 32]. The non-correlation among different templates of the same person using different keys is demonstrated in Section 5.2.3.

3.2.1 RP-RegSt

To generate the templates using the first proposed method, RP-RegSt, a new total scatter matrix from the vectors of $V = [v_{11}v_{12} \dots v_{N(m-1)}v_{Nm}]$ is formed as:

$$\hat{S}_t = \sum_{i=1}^{N} \frac{1}{n} \sum_{j=1}^{m} \left(v_{ij} - \bar{v}\right) \left(v_{ij} - \bar{v}\right)^T \tag{19}$$

where the column vector $v_{ij} \in \mathbb{R}^q$ in the matrix V represents the transformed cryptic pattern z_{ij}, $\bar{v} = \frac{1}{N} \Sigma_{i=1}^{N} \bar{v}_i$ represents the mean of all the column vectors of V, and $\bar{v}_i = \frac{1}{m} \Sigma_{j=1}^{m} v_{ij}$ represents the mean of transformed cryptic patterns of i^{th} class. The eigendecomposition is then applied to $\widehat{S}_t$ to extract the eigenvectors $\Omega_t \in \mathbb{R}^{q \times q}$ and eigenvalues Λ_t. After sorting the eigenvectors of Ω_t in decreasing order of the associated eigenvalues in Λ_t, the dimensionality reduction is performed by choosing the first k eigenvectors $\hat{\Omega}_t \in \mathbb{R}^{q \times k}$ where $k << q$. The regularized transformation matrix $F_t \in \mathbb{R}^{q \times k}$ following [25] is constructed as follows:

$$F_t = \tilde{\Omega}_w \hat{\Omega}_t \tag{20}$$

Finally, the template matrix for all persons is generated as follows:

$$T_t = F_t^T Z \tag{21}$$

where $T_t = \left[t_{11}, t_{12}, \ldots, t_{N(m-1)}, t_{Nm}\right] \in \mathbb{R}^{k \times n}$. The column vector t_{ij} represents the template corresponding to the biometric image x_{ij}.

3.2.2 RP-RegSb

The templates using the proposed method RP-RegSb are generated similarly to RP-RegSt, except that we construct a between-class scatter matrix instead of a total scatter matrix using transformed matrix V as follows:

$$\hat{S}_b = \sum_{i=1}^{N} \frac{1}{N} (\bar{v}_i - \bar{v})(\bar{v}_i - \bar{v})^T \tag{22}$$

The reduced set of weights $\hat{\Omega}_b$ can be obtained after the eigendecomposition of $\hat{S}_b$ followed by the selection of first k eigenvectors associated with the first k eigenvalues after sorting in decreasing order of Λ_b. Similar to equation (20), the regularized transformation matrix $F_b \in \mathbb{R}^{q \times k}$ following [25] is constructed as follows:

$$F_b = \tilde{\Omega}_w \hat{\Omega}_b \tag{23}$$

The templates for all persons using RP-RegSb are generated as follows:

$$T_b = F_b^T Z \tag{24}$$

These templates are non-invertible as only k features represent all q features and $k << q$. In the enrollment phase, a personalized key (a positive number) is assigned to each person (the person can also choose a key), determining the corresponding random permutation matrix. This random permutation matrix is used to transform the biometric images into cryptic patterns. The cryptic patterns are then converted into cancelable templates. These templates are stored in the database. In the authentication phase, the query image presented to the system (with key) is converted into the cancelable template using the same method, which will then be matched with the stored templates. The person must enter the correct key because a wrong key with the correct biometrics will result in a mismatch. If the template is matched, access to the system is granted. Otherwise, it is rejected. If the template of any person is stolen, then new templates can be issued by changing the personalized key. The personalized keys are stored in the database using some encryption techniques.

3.3 Improved Classification Accuracy using Random Permutation

Let $T: \mathbb{R}^q \rightarrow \mathbb{R}^q$ be a linear transformation. Now, the linear transformation T is defined as:

$$z_{ij} = T(x) = P_i x_{ij} \tag{25}$$

where P_i is the random permutation matrix, $x_{ij} \in \mathbb{R}^q$ is the column vector representing the biometric image, and $T(x) \in \mathbb{R}^q$ is the transformed column vector which is the randomly permuted x_{ij}. We can consider each column vector x_{ij} as a point in $q-$dimensional space. Therefore, this linear transformation transforms $x_{ij} \in \mathbb{R}^q$ to $z_{ij} \in \mathbb{R}^q$. This transformation can be seen as a projection of x_{ij} onto a different subspace. It is also given in the literature that samples from a specific object class are known to lie in the same linear subspace. Applying a class-specific permutation to the samples (biometric images) of different classes forms a distinct linear subspace for each individual. The distance between two linear subspaces increases, therefore enhancing the classification accuracy. The results of the experiments that prove the claim are shown in Subsection 5.1.2.

4 Experimental Setup and Biometric Databases

The proposed method is exhaustively tested on six publicly available biometric image databases. The list contains two face databases (Georgia Tech [33] and AT&T [34]), three iris (UBIRIS.v1 [35], CASIA-IrisV1 [36], IITD Iris [37]), and one ear database (IITD Ear [38]). Images with varying lighting conditions, positions, and other information can be found in biometric image databases. Each image is used without any pre-processing, except the Georgia Tech face database, where the color images were converted to grayscale before applying the proposed method. Each experiment is conducted on an HP Z2 Tower G5 workstation in Windows 11 and Python version 3.9.7. The biometric images of each person in the database are shuffled first before splitting into training and test sets. To avoid any randomness in the results, the seed given for shuffling the images of each person is three.

Table 1. Details of biometric image databases

Database	Original Dimension*	Dimension* Used	No. of Persons	Images per Persons
AT&T Face	92 × 112	92 × 112	40	10
Georgia Tech Face	640 × 480	100 × 75	50	15
UBIRIS-IrisV1	200 × 150	100 × 75	127	10
CASIA-V1 Iris	320 × 280	100 × 75	108	7
IITD Iris	320 × 240	100 × 75	224	10
IITD Ear	50 × 180	50 × 180	221	3

**width×height*

The images were resized and downsampled using the resize function of the OpenCV package. The random permutation matrices are generated by giving the user labels as seeds. User labels were integers beginning with zero and had to be entered in a sequence of images appearing in the database. Table 1 shows the details of the biometric databases used for the experiments.

Table 1 displays the original resolution, the resolution used for experiments, the number of persons, and the images per person for each database. AT&T [34] (formerly known as "The ORL Database of Faces") images have 256 grayscale levels and were initially stored in the original database in PGM file format but converted to JPG format before applying the methods. In Georgia, Tech [33], the frontal and angled faces are depicted with various scales, positions, and facial expressions. The color face images were converted to grayscale before using the template-generating techniques.

There are 1877 images in the UBIRIS.v1 Iris database [35] taken from 241 individuals at two separate sessions. Many noise elements were present in the collected images, which can be used to assess the robustness of the methods. The database initially had images of 241 and 132 people in the first and second sessions. 127 persons' iris images present in both sessions were used in the research; each person had ten or eleven images. Before experimenting, the eleventh image was removed for uniformity. In the CASIA-IrisV1 database [36], three images were captured in the first session, while four in the second. Before experimenting, images from both sessions were combined and converted to JPG format from BMP. The left eye images of 176 boys and 48 females between the ages of 14 and 55 can be found in the IITD Iris database [37]. Images were taken in a non-touching indoor setting for the IITD Ear [38]. Before starting the experiment, the pictures of CASIA-IrisV1, IITD Iris, and IITD Ear were converted from the original bitmap file format (BMP) into JPG.

5. Results Analysis

The templates were generated using the suggested procedures and underwent thorough performance and security analysis. The performance analysis discusses the suggested methods' recognition performance (given in Subsection 5.1), whereas the security analysis analyses the generated templates' quality and security (given in Subsection 5.2).

5.1 Performance Analysis

The classification accuracy is used to assess and compare our proposed methods with other competing methods. The number of training images, image size, and other variables affect the classification accuracy [22]. The systems with high classification accuracy are considered better than others. The classification accuracy (CA) (in percentage) can be calculated as:

$$CA = \frac{t}{n} \times 100 \qquad (26)$$

where t is the number of templates correctly classified, and n is the total number of templates in the test set. We used the K-nearest neighbors (KNN) technique for template classification, specifically with one neighbor for all competing and proposed methods. The k-nearest neighbor algorithm from the inbuilt package sklearn of Python is used. Cross-validation is employed to mitigate the influence of random variability on the test results. In Subsection 5.1.1, we assessed the effectiveness of the suggested procedures compared to alternative methods based on random permutations. The next subsection (5.1.2) examines the effect of applying random permutation on classification accuracy.

5.1.1 Classification Accuracy Comparision

The classification accuracy of the proposed method is compared with RP-PCA [3], RPLDA [21], and RP-LPP [22] approaches. These approaches have been developed to generate cancelable biometric templates using random permutations.

Table 2. Comparison of Classification Accuracy

Database ↓ # of Features →	RP-RegSt		RP-RegSb		RP-PCA		RPLDA		RP-LPP	
	10	20	10	20	10	20	10	20	10	20
AT&T Face	95.56	98.56	95.56	98.5	80.12	92.81	35.25	42.56	79.38	93.62
Georgia Tech Face	93.7	94.1	93.73	94.23	93.63	93.9	75.53	82.23	93.27	93.9
UBIRIS.v1 Iris	96.16	97.97	96.38	98.15	83.13	91.81	61.44	77.74	87.13	93.25
IITD Iris	94.13	98.39	94.27	98.36	87.82	95.79	22.54	42.38	92.06	97.19
Casia-IrisV1	95.37	98.21	95.62	98.33	84.32	93.95	43.21	63.09	88.09	95.25
IITD Ear	94.87	98.49	93.97	98.04	46.76	65.46	55.66	71.49	55.2	75.72

-*classification accuracies are given in percentage (%).

Based on our literature knowledge the above-mentioned methods have been chosen for comparison as they are the most recent and high-performing random permutation-based strategies on the AT&T, UBIRIS, and IITD Ear datasets for cancelable template generation. In RP-PCA and RP-LPP, the dimensionality is reduced using principal component analysis (PCA) and locality-preserving projection (LPP). The resulting reduced feature dimensions are referred to as components. However, in RPLDA, the dimension is reduced using linear discriminant analysis (LDA), and the features are referred to as discriminants. In the proposed method, the reduced features are also called discriminates. We use the term *features* to compare all methods. Biometric modality-wise comparison of recognition accuracy is discussed in the following subsections. The classification accuracy of *RP-RegSt* and *RP-RegSb* with other competing methods is given in Table 2.

5.1.1.1 Face

Two face databases are used to evaluate the performance of the proposed methods. Figure. 1 shows the classification accuracy comparison on AT&T face [34] and Georgia Tech face [33].

AT&T Face: Out of ten images, we trained the models of all competing approaches using two template images and assessed their performance using eight images of faces. The comparison of the classification accuracy of the proposed methods with other competing methods on AT&T

Face images is shown in Figure. 1a. It is visible that the performance of both the RP-RegSt and Rp-RegSb surpasses the performance of other methods. Both proposed methods, RP-RegSt and Rp-RegSb, achieve a significant classification accuracy of 95.56% for only ten features. And for 20 features, RP-RegSt achieves 98.56%, and Rp-RegSb achieves 98.5%. Acknowledging that RP-LPP and RP-PCA achieve comparable performance parity with RP-RegSt and Rp-RegSb, specifically when the feature count approaches 20.

Georgia Tech (GT) Face: The comparison of the classification accuracy on the GT face database is shown in Figure. 1b. This database contains 15 face images per person. We used three template images to train all the models for this database, and 12 biometric images were used to test the model's performance. The performance of all the competing methods except RPLDA is comparable with RP-RegSt and RP-RegSb on the GT face images, especially for more than ten features. For only ten features, the classification accuracy achieved by RP-RegSt is 93.7%, and RP-RegSb is 93.73%. The classification accuracy of RP-RegSt and RP- RegSb on 20 features is 94.1% and 94.23%, respectively.

5.1.1.2 Iris

For the iris biometric modality, two template images train the models of all competing methods. It is important to note that the proposed methods achieve more than 90% of classification accuracy for 10 features on all three iris databases.

UBIRIS.v1 Iris: The classification accuracy of all the methods on UBIRIS iris images is plotted against the number of features in Figure. 2a. Eight iris images out of ten are used to evaluate the models of all competing methods. The suggested techniques show a substantial difference in classification accuracy compared to all other competing methods. The classification accuracy of RP-RegSt and RP-RegSb for ten features is 96.16% and 96.38%, respectively. The RP-PCA, RP-LPP, and RPLDA could achieve only 83.13%, 87.13%, and 61.44%, respectively. For 20 features, the recognition accuracy obtained by RP-RegSt is 97.97%, and RP-RegSb is 98.15%.

***IITD Iris*:** Figure. 2b compares the performance of all five methods on the IITD Iris database.

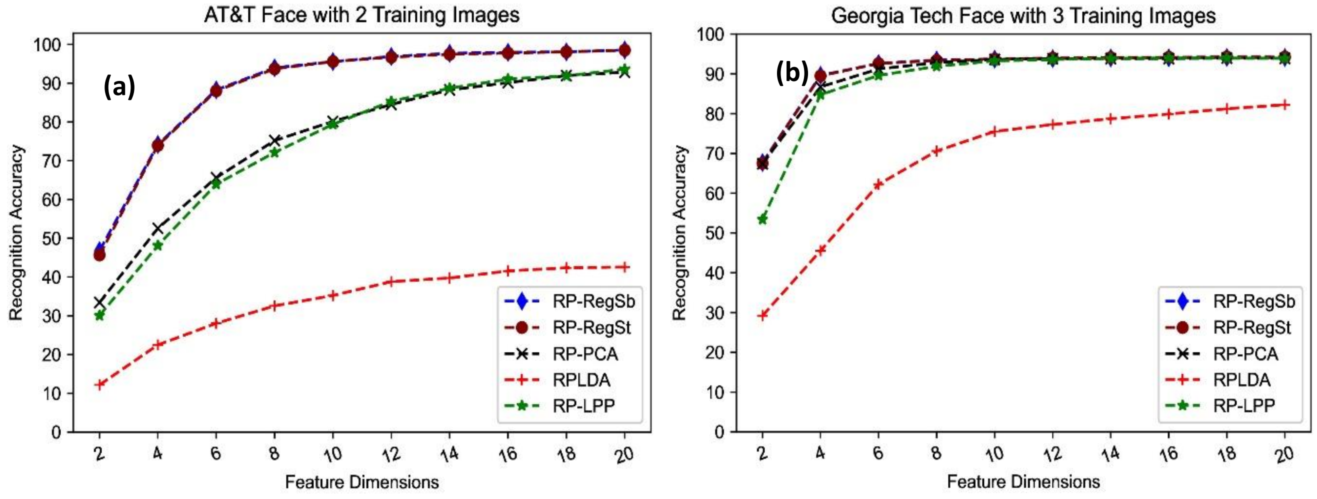

Figure 1. Classification Accuracy Comparison **(a)** AT&T Face and **(b)** Georgia Tech Face

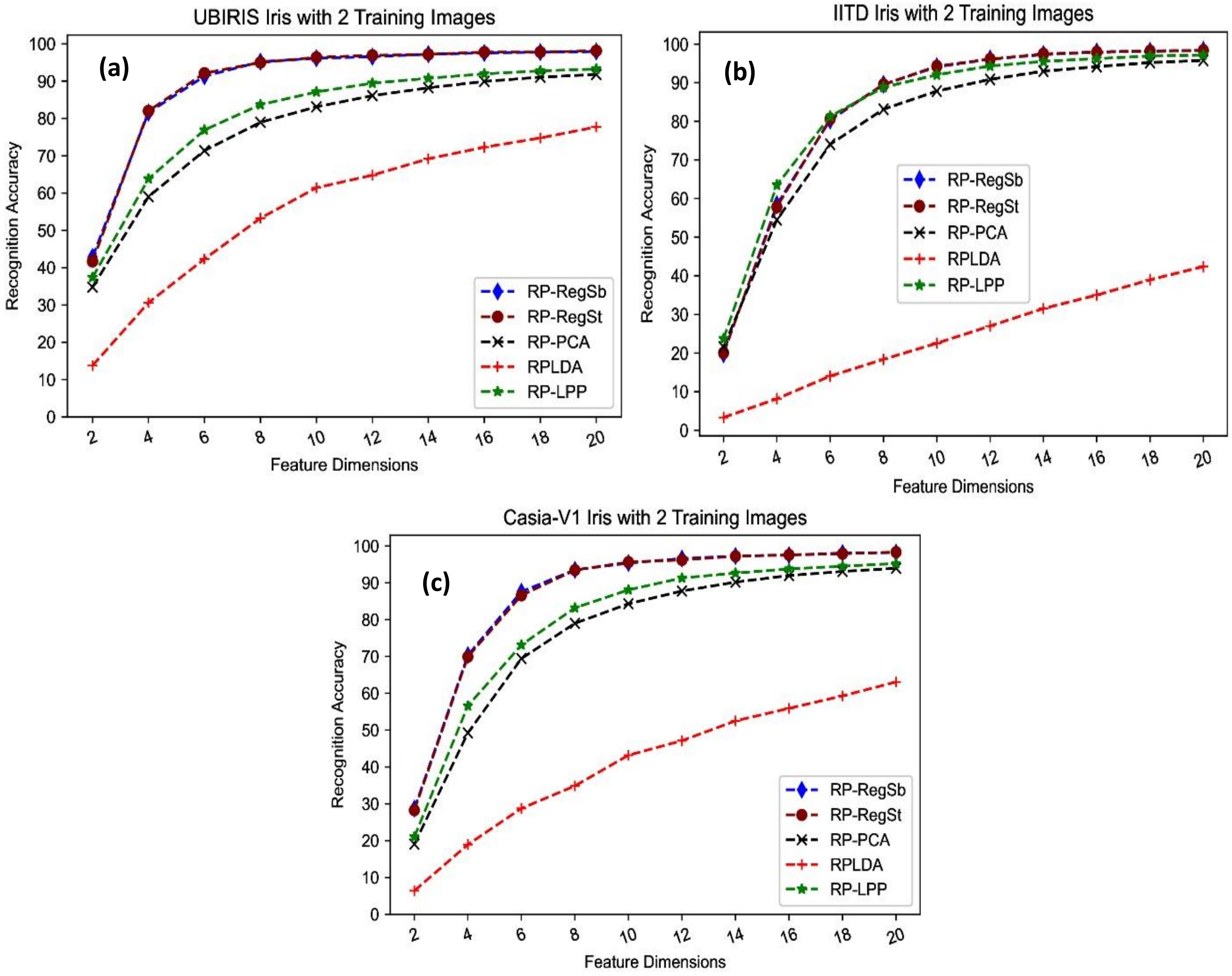

Figure 2. Classification Accuracy Comparison **a)** UBIRIS.v1, **b)** IITD Iris, **c)** CASIA-IrisV1

Out of 10, eight images were used in the testing phase, similar to UBIRIS.v1. The performance of RP-RegSt and RP-RegSb are almost similar, irrespective of the number of features. The performance of RP-LPP is comparable to that of the proposed methods, whereas RP-PCA performed a little lower. RPLDA couldn't perform well on the IITD Iris database images. RP-RegSt achieved 94.13% classification accuracy with ten features, and RP-RegSb achieved 94.27%. For 20 features, RP-RegSt and RP-RegSb achieved 98.39% and 98.36%, respectively.

Casia-IrisV1: The comparison of the performance of RP-RegSb and RP-RegSt with other methods on Casia-IrisV1 iris database is given in Figure. 2c. For this database, the test set comprises five images out of seven per individual. It can be easily observed that the classification accuracy obtained by RP-RegSt and RP-RegSb is better than that of other methods. For ten features only, RP-RegSt and RP-RegSb achieve an accuracy of 95.37% and 95.62%, respectively. For 20 features, the RP-RegSt method achieves 98.21% classification accuracy, while RP-RegSb achieves 98.33%.

5.1.1.3 Ear

For *IITD Ear* database, two images out of three are used to train all the models, and one is used for testing. Figure. 3 shows the performance comparison of all comparing methods on the ear database. It is crucial to note that none of the other approaches could provide results comparable to those of the proposed methods. The classification accuracy of RP-RegSt and RP-RegSb on ten features are 94.87% and 93.97%, respectively; for 20 features, it is 98.49% and 98.04%.

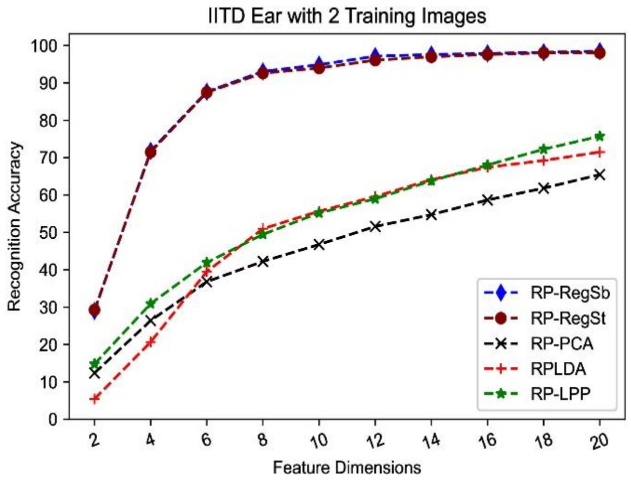

Figure 3. Classification Accuracy Comparison IITD Ear

5.1.2 Impact of Random Permutation on Recognition Accuracy

The experiments are conducted on all six biometric databases to check the effect of applying random permutation on the classification of biometric images. Table 3 shows the classification accuracy at ten features only. Every biometric dataset's training and test sizes are similar to those in Section 5.1.1. In row 1 and row 3, the results of classification using Regularized Total-Scatter (ERE_{St}) and Regularized between Scatter (ERE_{Sb}) are shown, whereas in row 2 and row 4, the results of classification using Random Permutation with Regularized Total-Scatter (RP-RegSt) and Random Permutation with Regularized Between-Scatter (RP-RegSb) are displayed.

The data presented in Table 3 demonstrates that using random permutations with eigenfeature regularisation has a notable positive impact on the classification accuracy of each biometric database. Out of both proposed methods, the RP-RegSb approach demonstrated the minimum increase in classification accuracy of 3.43%, increasing the accuracy on the GT face database from 90.3% to 93.73%. The RP-RegSt approach demonstrated a maximum increase in classification accuracy of 32.9% on Casia-IrisV1, increasing the accuracy from 62.47% to 95.37%. The RP-RegSb algorithm shows an average increase in classification accuracy of 17.11% across all biometric datasets, while the RP-RegSt algorithm demonstrates a 19.49% average increase. This improvement can be considered noteworthy. Therefore, it is proved that classification accuracy improves when random permutation is applied.

5.2 Privacy and Security Analysis

This subsection provides a detailed privacy and security analysis of the templates generated using proposed methods. We demonstrate that the templates fulfil the other three fundamental characteristics of cancelable biometrics: non-invertibility (security), diversity, and revocability, in addition to performance. Figure 4. contains three images for each database, where the first image represents an original biometric image of a random person, and the second and the third images are their corresponding templates generated by the proposed methods RP-RegSt and the RP-RegSb, respectively. It is visible from the template images that they are dissimilar to the original image and reveal no visual information about the original biometric data. The security of the templates is demonstrated through brute force attack analysis.

5.2.1 Non-Invertibility Analysis

The concern of privacy analysis is directly related to the invertibility of the transformed template. Non-invertibility, or irreversibility, refers to the inability to retrieve the original biometric information from the generated template. There may be two scenarios using which an adversary wants to perform this retrieval. In the first scenario, the adversary only has access to the template without the key. In contrast, in the second scenario, the adversary can access both the template and the key. In the first scenario, recovering biometric information from the template without the key requires two steps: a) transform the template into the cryptic pattern and b) transform the cryptic pattern into original biometric information. In the second scenario, the adversary only needs to convert the template into its corresponding cryptic pattern because the original biometric image can be directly generated from the cryptic pattern using the key by taking the inverse of the random permutation matrix.

Let us first discuss the latter scenario, where the adversary has the key and the template.

Table 3. Effect of Random Permutation on Classification Accuracy* at Ten Features

Row No.	Method	ORL	GT	UBIRIS	IITD Iris	Casia	IITD Ear
1	ERE$_{St}$	81.62	89.33	78.54	65.79	62.47	75.11
2	RP-RegSt	95.56	93.7	96.16	94.13	95.37	94.87
3	ERE$_{Sb}$	82.12	90.3	79.96	69.2	63.83	81.45
4	RP-RegSb	95.56	93.73	96.38	94.27	95.62	93.97

*Classification accuracies are given in percentage (%).

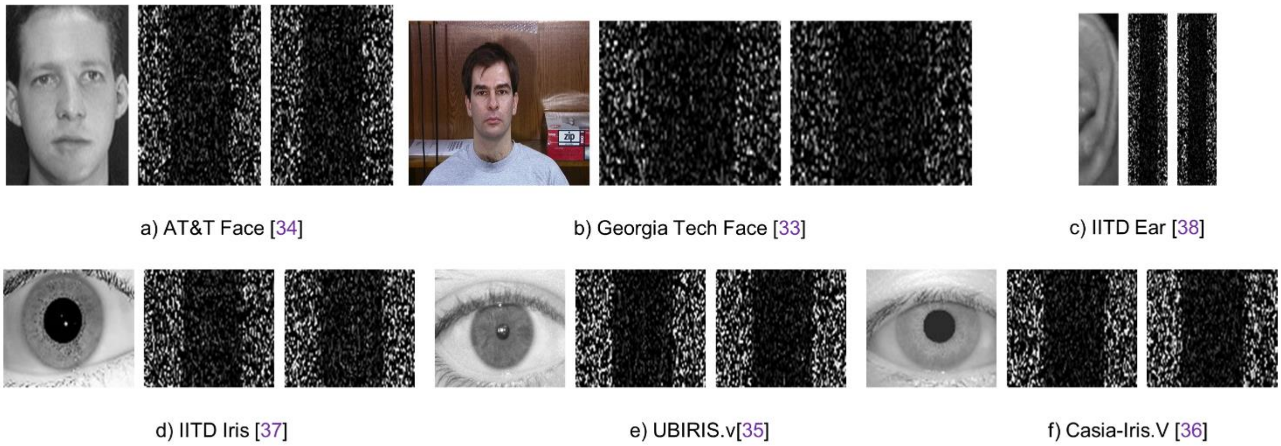
a) AT&T Face [34]
b) Georgia Tech Face [33]
c) IITD Ear [38]
d) IITD Iris [37]
e) UBIRIS.v[35]
f) Casia-Iris.V [36]

Figure 4. Sample Image, RP-RegSb Template, and RP-RegSt Template from six Databases

The templates are visibly secure, as seen in Figure 4. There is no similarity between the original biometric images and their corresponding templates. However, statistical experiments are essential to determine the level of the relationship or similarity between the created templates and the corresponding biometric image. Some metrics used in cancelable biometrics to check the similarity between two images are as follows [39, 40].

- Correlation coefficient (Cr): gives 0 if both the images are not related to each other, and the values 1 or -1 represent the positive or negative correlation, respectively,
- Mean Squared Error (MSE): an optimal value for a cancelable template should differ significantly from zero because the zero value represents a similar image,
- Structure SIMilarity ($SSIM$): value ranges between -1 and 1, where -1 and 1 represent different and same images, respectively. A value of 0 indicates no similarity.
- Number of Pixel Change Rate ($NPCR$): calculates the pixel percentage that differs in two images.
- Unified Average Changing Intensity ($UACI$): provide the average difference in intensity between plain and encrypted images [41].

Table 4 describes the correlation and similarity metrics' formulas to assess the generated templates' quality. These metrics are used to compute the relationship between cryptic patterns and template images, and the results are given in Table 5.

The mean correlation values between the cryptic patterns and the templates approach zero, which implies a lack of correlation between the cryptic patterns and template images. Hence, it can be argued that the generated templates have no direct relationship with their cryptic patterns. The MSE between the cryptic patterns and their generated templates reaches thousands, and SSIM approaching zero proves they are dissimilar. An image encryption system is immune to different imposters attacks if the UACI (Unified Average Changing Intensity) is more than 33.4635% and the NPCR (Number of Pixel Change Rate) is greater than 99.6094% [42]. As displayed in Table 5, the outcomes for all databases show that the NPCR is 100% and the UACI is much higher than 33.4635%. The templates generated using RP-RegSt and RP-RegSb proved to have no relation with their cryptic patterns, as evidenced by the correlation coefficient, MSE, and SSIM. Consequently, these templates are secure and deemed resistant to impostor attacks, as evidenced by NPCR and UACI. Therefore, the results prove that the cryptic patterns are unrelated to their corresponding templates and immune to different imposters' attacks.

Applying random permutation to the biometric data also makes it secure [4]. If only the template (without the key) is compromised, then recovering the original biometric information from the cryptic pattern almost equals guessing the biometric image. In this case, for a q-dimensional column vector, n^q guesses are required in the worst case and $n^q/2$ in the average case. In our case, the n is 256, therefore $(2^8)^{9000}$ guesses are required in the worst case and $(2^8)^{9000}/2$ in the average case. In both cases, the complexity is $O(2^8)^{9000}$, which is very high. Therefore, converting cryptic patterns to the original biometric images is computationally impossible without the key, and hence, guessing a random array of such high dimensions is difficult.

It has been proved that the generated template is safe from imposters' attacks and that the cryptic pattern cannot be recovered. Applying random permutation through personalized keys adds a layer of security to the template. Therefore, the generated templates are non-invertible in both scenarios, and the proposed method satisfies this characteristic of cancelable biometrics.

5.2.2 Brute Force Attack Analysis

In a brute force attack, the adversary tries all possible combinations to generate the transformed template [43]. If the adversary knows the transform function, he/she must have the cryptic pattern to transform it into the template. Since, the cryptic patterns are constructed by applying random permutation on the column vector representing the original biometric image, the $q!$ iterations are required to create a q-dimensional cryptic pattern in the absence of the user-specific key, where $q = width \times height$. According to Table 1 a minimum of $9000!$ iterations are necessary to produce the cryptic pattern, making the computational task exceedingly challenging. Even the fastest supercomputer with a speed of 10^{17} floating point operations per second (FLOPS) would take thousands of centuries to create the cryptic pattern. Therefore, the templates are secured from brute force attacks.

5.2.3 Diversity and Revocability Analysis

The diversity criterion in cancelable biometrics requires that the templates representing the same biometrics should not be associated with one another across different applications. The lack of correlation between the randomly generated keys guarantees that the templates created using various keys are not correlated [8].

This enables using distinct keys for multiple applications or systems. Therefore, in the proposed methods, different templates can be generated using separate keys for the various applications for the same person. Hence, the requirement of diversity is met.

For revocability requirements, another template may be quickly generated by simply changing the key if the template or the key is compromised. The changed key produces a new permutation matrix, which, as a result, generates a new cancelable template that would be uncorrelated with the stolen one [31]. This process creates new templates for specific users without affecting the templates of other users. It demonstrates the accomplishment of the crucial revocability/ renewability characteristic.

Table 4. Correlation and Similarity Metrics

Formula	Description
$C_r(B,T) = \dfrac{\sum_i \sum_j \ (B_{ij}-\overline{B})(T_{ij}-\overline{T})}{\sqrt{\left(\sum_i \ \sum_j \ (B_{ij}-\overline{B})^2\right)\left(\sum_i \ \sum_j \ (T_{ij}-\overline{T})^2\right)}}$	B_{ij} and T_{ij} are the biometric and template images, respectively. $\overline{B}$ and $\overline{T}$ the mean of B or T.
$MSE = \dfrac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (B(i,j) - T(i,j))^2$	W and H are the number of pixels in width and height, respectively
$SSIM(B,T) = \dfrac{(2\mu_B\mu_T + C_1)(2\sigma_{BT} + C_2)}{(\mu_B^2 + \mu_T^2 + C_1)(\sigma_B^2 + \sigma_T^2 + C_2)}$	μ_i is the mean, σ_i is the variance, σ_{BT} is the covariance of *B* & *T*, and C_i is the constant
$NPCR = \dfrac{\sum_{i,j} D(i,j)}{W \times H} \times 100$	$D(i,j) = 1$ if the corresponding pixels of two images are different and *0* otherwise
$UACI = \dfrac{1}{W \times H} \times \left(\dfrac{\sum_{i,j} B(i,j) - T(i,j)}{255}\right) \times 100$	*255* is the maximum intensity value of a pixel in the grayscale image

Table 5. Correlation and Similarity Analysis

Database	Method	Correlation	MSE	SSIM	NPCR	UACI
AT&T Face	Template-St	0.0086	29989.11	0.0026	100	56.96
	Template-Sb	0.0051	30063.32	0.0031	100	56.93
Georgia Tech Face	Template-St	0.0139	15285.88	0.0021	100	39.16
	Template-Sb	0.0042	15284.37	-0.0027	100	39.02
UBIRIS.v1 Iris	Template-St	-0.0154	51322.67	-0.0014	100	76
	Template-Sb	-0.0163	53325.47	-0.0026	100	77.49
Casia-IrisV1	Template-St	0.0048	45818.11	0.005	100	71.59
	Template-Sb	0.0115	40145.32	0.0063	100	65.62
IITD Iris	Template-St	0.0021	40535.21	0.0029	100	66.35
	Template-Sb	0.0115	40145.32	0.0063	100	65.62
IITD Ear	Template-St	0.0018	19332.69	0.0034	100	46.64
	Template-Sb	-0.0022	20073.65	0.0023	100	47.31

6 Conclusion and Future Work

This research proposes two cancelable biometric generation methods (*RP-RegSt & RP-RegSb*) for authentication. The templates are generated by applying random permutation with eigenfeature regularization and feature extraction (ERE). The personalized key seeds a random permutation matrix that converts the biometric image into a cryptic pattern. The eigenfeatures of the cryptic pattern are regularized using ERE. These regularized eigenfeatures transform the cryptic pattern into a cancelable template using a between-class or total scatter matrix. We exploit the discriminative and stable low-dimensional feature representation advantage of eigenfeature regularization and feature extraction (ERE) to enhance recognition accuracy and save storage space. Since the training phase generates the transformation matrix, the regularization process takes a little longer than PCA and LDA, but this is acceptable and does not affect the testing time. Privacy concerns are effectively addressed as the templates are irreversible and secure from imposters' attacks. If a user's template, key, or both are compromised, then new templates are generated by quickly changing the personalized key, like passwords. The proposed approaches satisfy the diversity (unlinkability) property, allowing us to use them for different applications for the same persons. The brute force analysis shows that the security concern is also resolved. Both approaches adhere to the key properties of cancelable biometrics, making it a promising approach for secure biometric authentication. This study also indicates that the recognition performance of the cancelable template generation algorithms improves by applying random permutations. The suggested approaches outperformed other state-of-the-art random permutation-based cancelable template generation methods on six biometric datasets.

This study might be extended to develop cancelable biometric templates for other biometrics beyond face, iris, and ear biometric images. Future research might focus on multi-modal biometrics, which uses more than one biometric modality for authentication.

References

[1] Farooq, R.M. Bolle, T.Y.Jea, N. Ratha, (2007) Anonymous and revocable fingerprint recognition. In 2007 IEEE Conference on Computer Vision and Pattern Recognition, IEEE, USA. https://doi.org/10.1109/CVPR.2007.383382

[2] S. Veerashetty, Virupakshappa, Ambika, Face recognition with illumination, scale and rotation invariance using multiblock ltp-glcm descriptor and adaptive ann. International Journal of System Assurance Engineering and Management, 15(1), (2024) 174–187. https://doi.org/10.1007/s13198-022-01688-0

[3] N. Kumar, S. Singh, A. Kumar, Random permutation principal component analysis for cancelable biometric recognition. Applied Intelligence, 48, (2018) 2824–2836. https://doi.org/10.1007/s10489-017-1117-7

[4] J.C. Bernal-Romero, J.M. Ramirez-Cortes, J.D.J. Rangel-Magdaleno, P. Gomez-Gil, H. Peregrina-Barreto, I. Cruz-Vega, A review on protection and cancelable techniques in biometric systems. IEEE Access, 11, (2023) 8531–8568. https://doi.org/10.1109/ACCESS.2023.3239387

[5] N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3), (2001) 614–634. https://doi.org/10.1147/sj.403.0614

[6] A.B.J. Teoh, C.T. Yuang, Cancelable biometrics realization with multispace random projections. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 37(5), (2007) 1096–1106. https://doi.org/10.1109/TSMCB.2007.903538

[7] S. Cho, A.B.J. Teoh, Face template protection via random permutation maxout transform. In: Proceedings of the 2017 International Conference on Biometrics Engineering and Application. ICBEA' 17, (2017) 21–27. https://doi.org/10.1145/3077829.3077833

[8] D.H. Lee, S.H. Lee, N.I. Cho, (2018) Cancelable biometrics using noise embedding. In: 2018 24th International Conference on Pattern Recognition (ICPR), IEEE, China. https://doi.org/10.1109/ICPR.2018.8545121

[9] V.S. Baghel, S.S. Ali, S. Prakash, A noninvertible transformation based technique to protect a fingerprint template. IET Image Processing, 17(13), (2023) 3645–3659. https://doi.org/10.1049/ipr2.12130

[10] A. Sarkar, B. Singh, A cancelable biometric based secure session key agreement protocol employing elliptic curve cryptography. International Journal of System Assurance Engineering and Management, 10(5), (2019) 1023–1042. https://doi.org/10.1007/s13198-019-00832-7

[11] N. Manisha, Kumar, Cancelable biometrics: A comprehensive survey. Artificial Intelligence Review 53, (2020) 3403–3446. https://doi.org/10.1007/s10462-019-09767-8

[12] N. Kumar, A. Jaiswal, R.K. Agrawal, Performance evaluation of subspace methods to tackle small sample size problem in face recognition. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics. ICACCI', (2012) 938–944. https://doi.org/10.1145/2345396.2345547

[13] M. Turk, A. Pentland, Eigenfaces for Recognition. Journal of Cognitive Neuroscience, 3(1), (1991) 71–86. https://doi.org/10.1162/jocn.1991.3.1.71

[14] P.N. Belhumeur, J.P. Hespanha, D.J. Kriegman, Eigenfaces vs. fisherfaces: recognition using class specific linear projection. IEEE Transactions on Pattern Analysis and Machine Intelligence 19(7), (1997) 711–720. https://doi.org/10.1109/34.598228

[15] B. Moghaddam, T. Jebara, A. Pentland, Bayesian face recognition. Pattern Recognition, 33(11), (2000) 1771–1782. https://doi.org/10.1016/S0031-3203(99)00179-X

[16] J. Kim, J. Choi, J. Yi, M. Turk, Effective representation using ica for face recognition robust to local distortion and partial occlusion. IEEE Transactions on Pattern Analysis and Machine Intelligence 27(12), (2005) 1977–1981. https://doi.org/10.1109/TPAMI.2005.242

[17] T.K. Kim, H. Kim, W. Hwang, J. Kittler, Independent component analysis in a local facial residue space for face recognition. Pattern Recognition, 37(9), (2004)1873–1885. https://doi.org/10.1016/j.patcog.2004.01.019

[18] X. He, P. Niyogi, (2003) Locality preserving projections. In: Proceedings of the 16th International Conference on Neural Information Processing Systems. NIPS'03, MIT Press, Cambridge, USA.

[19] D. Zhou, X. Yang, N. Peng, Y. Wang, Improved-lda based face recognition using both facial global and local information. Pattern Recognition Letters, 27(6), (2006) 536–543. https://doi.org/10.1016/j.patrec.2005.09.015

[20] A. Jaiswal, R.K. Agrawal, N. Kumar, Performance evaluation of linear subspace methods for face recognition under illumination variation. C3S2E '11: Proceedings of the Fourth International C* Conference on Computer Science and Software Engineering, (2011) 103–110. https://doi.org/10.1145/1992896.1992909

[21] P. Punithavathi, S. Geetha, (2021) Random permutation-based linear discriminant analysis for cancelable biometric recognition. Advances in Computing and Network Communications, Springer, Singapore. https://doi.org/10.1007/978-981-33-6977-1_43

[22] N. Kumar, M. Rawat, Rp-lpp: a random permutation based locality preserving projection for cancelable biometric recognition. Multimedia Tools and Applications 79, (2020) 2363–2381. https://doi.org/10.1007/s11042-019-08228-2

[23] H. Yu, J. Yang, A direct lda algorithm for high-dimensional data-with application to face recognition. Pattern Recognition, 34(10), (2001) 2067–2070. https://doi.org/10.1016/S0031-3203(00)00162-X

[24] W. Liu, Y. Wang, S.Z. Li, T. Tan, (2004) Null space approach of fisher discriminant analysis for face recognition. Biometric Authentication, Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-25976-3_4

[25] X. Jiang, B. Mandal, A. Kot, Eigenfeature regularization and extraction in face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 30(3), (2008) 383–394. https://doi.org/10.1109/TPAMI.2007.70708

[26] V.M. Patel, N.K. Ratha, R. Chellappa, Cancelable biometrics: A review. IEEE Signal Processing Magazine 32(5), (2015) 54–65. https://doi.org/10.1109/MSP.2015.2434151

[27] J. Zuo, N.K. Ratha, J.H. Connell, (2008) Cancelable iris biometric. In: 2008 19th International Conference on Pattern Recognition, IEEE, USA. https://doi.org/10.1109/ICPR.2008.4761886

[28] A.B.J. Teoh, S. Cho, J. Kim, Random permutation maxout transform for cancellable facial template protection. Multimedia Tools and Applications, 77, (2018) 27733–27759. https://doi.org/10.1007/s11042-018-5956-y

[29] O. Singh, A. Jaiswal, N. Kumar, N. Kumar, Random permutation-based linear regression for cancelable biometrics. Expert Systems, 42(2), (2024) 13652. https://doi.org/10.1111/exsy.13652

[30] A.M. Martinez, A.C. Kak, Pca versus lda. IEEE Transactions on Pattern Analysis and Machine Intelligence, 23(2), (2001) 228–233. https://doi.org/10.1109/34.908974

[31] Z. Shao, L. Li, Z. Zhang, B. Li, X. Liu, Y. Shang, B. Chen, Cancelable face recognition using phase retrieval and complex principal component analysis network. Machine Vision and Applications 35(1), (2024) 12. https://doi.org/10.1007/s00138-023-01496-x

[32] Naseem, R. Togneri, M. Bennamoun, Linear regression for face recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence 32(11), (2010) 2106–2112. https://doi.org/10.1109/TPAMI.2010.128

[33] A.V. Nefian, (2020). Georgia tech face database 1999.

[34] F.S. Samaria, A.C. Harter, Parameterisation of a stochastic model for human face identification. In: Proceedings of 1994 IEEE Workshop on Applications of Computer Vision, IEEE, USA. https://doi.org/10.1109/ACV.1994.341300

[35] H.Proenca, L.A. Alexandre, Ubiris: A noisy iris image database. Image Analysis and Processing – ICIAP 2005, Springer, Berlin. https://doi.org/10.1007/11553595_119

[36] Casia.V1: Casia-IrisV1 database. http://biometrics.idealtest.org/

[37] A. Kumar, A. Passi, Comparison and combination of iris matchers for reliable personal authentication. Pattern Recognition, 43(3), (2010) 1016–1026. https://doi.org/10.1016/j.patcog.2009.08.016

[38] A. Kumar, C. Wu, Automated human identification using ear imaging. Pattern Recognition 45(3), (2012) 956–968. https://doi.org/10.1016/j.patcog.2011.06.005

[39] N. Manisha, Kumar, on generating cancelable biometric template using reverse of boolean xor. In: 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3), (2020) 1-4.

[40] N. Kumar, Manisha, Cbrw: a novel approach for cancelable biometric template generation based on 1-d random walk. Applied Intelligence, 52(13), (2022) 15417–15435.

[41] Y. Wu, J.P. Noonan, S. Agaian, Npcr and uaci randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 1(2), (2011) 31–38.

[42] M. Essaid, I. Akharraz, A. Saaidi, A. Mouhib, A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map. Procedia Computer Science, 127, (2018) 539–548. https://doi.org/10.1016/j.procs.2018.01.153

[43] M.J. Lee, A.B.J. Teoh, A. Uhl, S.N. Liang, Z. Jin, A tokenless cancellable scheme for multimodal biometric systems. Computers & Security, 108, (2021) 102350. https://doi.org/10.1016/j.cose.2021.102350

Authors Contribution Statement

Onkar Singh: Conceptualization, Methodology, Software, Validation, and Writing Original Manuscript. Ajay Jaiswal: Conceptualization, Methodology, Validation and Manuscript Review. Nitin Kumar: Validation and Manuscript Review. Naveen Kumar: Validation and Manuscript Review. All authors read and approved the final manuscript.

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

We are thankful to the following authors/academies for providing the following biometric databases, which were instrumental in conducting our research:

CASIA-IrisV1: Portions of the research in this paper use the CASIA-IrisV1 collected by the Chinese Academy of Science's Institute of Automation (CASIA). *Database Link*: http://biometrics. idealtest.org/

UBIRIS.v1: Proen¸ca, Hugo, and Alexandre, Lu´ıs A., *Database Link*: http://iris.di.ubi.pt/ubiris1. html

IITD Iris and IITD Ear: Prof. Ajay Kumar, *IITD Iris Database Link*: https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm and *IITD Ear Database Link*: https://www4.comp.polyu.edu.hk/~csajaykr/IITD/Database_Ear.htm

AT&T Face: Samaria, F.S., Harter, A.C., *Database Link*: https://cam-orl.co.uk/facedatabase.html

Georgia Tech Face: Dr. Ara V. Nefian, *Database Link*: https://www.anefian.com/research/ face reco.htm

Has this article screened for similarity?

Yes

About the License