



RP-LPP : a random permutation based locality preserving projection for cancelable biometric recognition

Nitin Kumar¹  · Manisha Rawat¹

Received: 24 December 2018 / Revised: 21 July 2019 / Accepted: 13 September 2019 /

Published online: 20 November 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

Biometrics are being increasingly used across the world, but it also raises privacy and security concerns of the enrolled identities. The main reason is due to the fact that biometrics are not cancelable and if compromised may give access to the intruder. Cancelable biometric template is a solution to this problem which can be reissued if compromised. In this paper, we suggest a simple and powerful method called Random Permutation Locality Preserving Projection (RP-LPP) for Cancelable Biometric Recognition. Here, we exploit the mathematical relationship between the eigenvalues and eigenvectors of the original biometric image and its randomly permuted version is exploited for carrying out cancelable biometric recognition. The proposed technique work in a cryptic manner by accepting the cancelable biometric template and a key (called PIN) issued to a user. The effectiveness of the proposed techniques is demonstrated on three freely available face (ORL), iris (UBIRIS) and ear (IITD) datasets against state-of-the-art methods. The advantages of proposed technique are (i) the classification accuracy remains unaffected due to cancelable biometric templates generated using random permutation, (ii) security and quality of generated templates and (iii) robustness across different biometrics. In addition, no image registration is required for performing recognition.

Keywords Cryptic · Revocable · PIN · Single sample

The corresponding author is thankful to Uttarakhand State Council for Science and Technology, Dehradun, Uttarakhand, India for providing financial support towards this research work (Sanction No. UCS&T/R&D-05/18-19/15202/1 dated 28-09-2018)

✉ Nitin Kumar
nitin@nituk.ac.in

Manisha Rawat
manisharawat615@gmail.com

¹ Department of Computer Science and Engineering, National Institute of Technology, Uttarakhand, Srinagar Garhwal, Uttarakhand, India

1 Introduction

Biometric [13, 36] is a combination of two words i.e. *bio* meaning life and *metrikos* meaning measurement. Thus, it can be defined as any physical and/or behavioral characteristic of a person which can uniquely identify a person or identity. There has been numerous applications of this concept in access control, border immigration control, corpse identification, surveillance, forensic sectors [36], human computer interaction [50], behavior analysis [6] *etc.* Due to these burgeoning applications of biometric system, researchers from various communities such as pattern recognition, statistics, machine learning, computer vision and so on have come together to solve this fascinating problem. In a typical biometric recognition system, a user presents his biometric such as face [50], fingerprint[34], iris[31], voice [9] *etc.* to the system and recognition is performed by matching the test entity against the stored representations. Biometric recognition is typically performed with the help of digital images captured by some biometric sensor such as camera. Since the biometric images involve high dimensions and only few samples for an identity are available for training, this leads to the problem of *curse of dimensionality* or *Small Sample Size (SSS)* [2] in literature.

SSS problem can be alleviated by either increasing the number of samples or by reducing the dimensions of the biometric image. Due to the intricacies involved in collection of biometric samples, this option is less feasible. On the other hand, it is viable to reduce the dimensions of biometric image using some dimension reduction technique. A comprehensive survey of linear dimensionality reduction techniques is carried out by Cunningham and Ghahramani [5]. Several techniques such as Locality Preserving Projection (LPP) [11], principal component analysis (PCA) [33], canonical correlation analysis (CCA) [12], Fisher's linear discriminant analysis [7], multidimensional scaling [4], slow feature analysis (SFA) [46, 47] *etc.* are presented in their research work [5]. It is shown that the linear dimensionality reduction can be modeled as a matrix optimization problem. Besides, some methods based on selection and weighting of facial features are also proposed in literature by Leng et al. [24, 25] in which weighted discrimination power analysis has been employed in Discrete Cosine Transform (DCT) domain for feature extraction. Locality Preserving Projection (LPP) is a simple and popular technique of dimensionality reduction in which the data points are assumed to lie on a high dimensional manifold. The objective in LPP is to find optimal linear approximation to the Eigenfunctions of the Laplace Beltrami operator on the manifold. LPP has been successfully applied in face and handwriting recognition [11], palm vein verification [1] *etc.*

With increasing popularity of the biometric systems, there has been a growing concern over security and privacy of people. This is due to the fact that biometrics are permanently associated with a person in contrast to credit cards and passwords which can be blocked and reissued when stolen. If the biometric pattern is stolen by some intruder, then it is highly probable that he can deceive the biometric recognition system and gain access to secure areas. To overcome these limitations, the concept of cancelable biometric [32] have been suggested in literature. In cancelable biometric, an individual is issued a biometric template which is subsequently used by that individual for recognition instead of the original biometric. If this template is stolen or compromised, the same can be reissued in the same way as credit card or password *etc.* Several techniques have been suggested for cancelable biometric template generation in literature. A comprehensive survey of cancelable biometric template generation is given by Patel et al. [32] in which cancelable biometric techniques have been broadly classified into ten categories *viz.* (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.

Noninvertible Geometric Transforms morph the biometric image by employing some transformation in signal or feature space [3, 38, 39]. The drawback of these methods is instability i.e. a small change in the original biometric may lead to large variations in generated biometric template after transformation thereby affecting the overall performance. In Random Projection Methods, a biometric template is projected to a lower dimension using a matrix whose elements are independently realized random variables. This matrix is chosen such that the distances between any two feature points is preserved in the transformed sample space. See [35] for details where some matrices are defined which satisfy these criteria. Two dimensional cancelable biometric methods [26, 29] have also been suggested under this category in which the whole biometric image is used as feature matrix instead of converting the original biometric image. Savvides et al. [42] suggested cancelable biometric filters where the original biometric images are convolved with user specific convolution kernel and these encrypted images are used to generate a filter called minimum average correlation energy (MACE). During enrollment, users are also assigned a personal identification number (PIN). The user presents the biometric template and PIN simultaneously to the system for recognition. Bioconvolving [30] is another biometric template generation method which is particularly applicable in scenarios where set of sequence can be employed to represent a biometric template e.g. signature. In this method, a key vector $\mathbf{d} = [d_0 \ d_1 \ \dots d_k]$ is formed such that $d_k > d_{k-1}$ and d_0 and d_k are set to 0 and 100 respectively. Based on this key, the original sequence is broken into k mutually exclusive segments. These segments are then linearly convoluted to obtain the transformed sequence. Recently, bloom filters [40] have also been successfully applied for biometric template generation. A bloom filter is a probabilistic data structure that supports membership queries on a set. The key advantage of these filters is that a high level of security is provided while much affect on the recognition accuracy. Behavioral biometrics such as voice is also vulnerable to be copied and misused. Knowledge signatures [49] is a scheme in which a person is allowed to sign on a group's behalf such that if the biometric is compromised, then it can not be identified exactly the person whose voice is represented by the biometric template. This scheme employs factorization of large integers and hence privacy of the user is protected. Biohashing [44] methods extend random projection methods where some feature extraction method such as wavelet transform is employed before computing the inner product with identity specific tokenized random number (TRN).

In most of the above categories, the recognition accuracy is negatively affected as the representation used for performing recognition is altered in order to ensure the privacy and security of the concerned individuals. Random permutation [35, 51] is another biometric template generation method and it encompasses only rearrangement of features and recognition accuracy is not much affected. Zuo et al. [51] have suggested four random permutation methods called GRAY-COMBO, BIN-COMBO, GRAY-SALT and BIN-SALT. In GRAY-COMBO, the original biometric is transformed by first shifting the rows circularly using random offsets and then adding the rows randomly. In BIN-COMBO, the same operation is performed on the iris codes by random shifting and XOR-ing. In GRAY-SALT, a completely artificial pattern equal to the size of original image is added to the original image to get the cancelable biometric image. In BIN-SALT, the artificial pattern is converted into binary pattern using a threshold and is added to the original pattern. Uhl et al. [10] have also suggested another random permutation method in which the original biometric image is first divided into rectangular patches and then these rectangular patches are permuted randomly to obtain the encoded biometric image.

There are some methods based on hash codes such as PalmHash Code [28], 2D PalmHash Codes [20, 22], PalmPhasor Code [23], 2-D PalmPhasor [27] etc. which have been effectively employed for cancelable biometric recognition. Here, Conjugate 2D PalmHash code [20] is used in multimodal scenario while other methods are employed in unimodal scenario. Another approach for addressing cancelable biometric system is based on biometric cryptosystem. A popular method under this category is suggested by Leng et al. [21] in which two hybrid cancelable palm print cryptosystems has been proposed based on palm print texture code, dubbed row-alone and row-co-occurrence Fuzzy Vaults. There are some other recent methods based on synthetic minutiae [8], Noise embedding [19], Index-of-Max Hashing [14], Random Distance [16], electrocardiogram (ECG) [48] which has been suggested for cancelable biometric template generation.

To address the issues of security and privacy of user's data and simultaneously achieving good recognition accuracy, in this paper, we propose a novel method called Random Permutation Locality Preserving Projection (RP-LPP). The main contribution of the work is two-fold:

- A novel method for cancelable biometric recognition based on Random Permutation (RP) and Locality Preserving Projection (LPP) is proposed.
- The mathematical relationship between the eigenvalues and eigenvectors of the original biometric image and its randomly permuted version is exploited for carrying out cancelable biometric recognition.

The rest of the paper is organized as follows: Section 2 provides a brief overview of the LPP algorithm. Section 3 presents the proposed method. In this section, we show how random permutations can be employed to generate encrypted biometric template and hence LPP is applied without affecting the classification accuracy. Experimental Setup is given in Section 4 while Results and Discussion are given in Section 5. Here, the analysis pertaining to the security of the biometric template, quality, classification accuracy and computational complexity of the proposed techniques is presented. Finally, conclusion of the research work is given in Section 6.

2 Locality preserving projection

Let $\mathbf{x} \in \mathbb{R}^d$ be a column vector representing an image in a d dimensional space and there are c identities $\{1, 2, 3, \dots, c\}$ such that each identity has N_i images. Thus, total number of training images is $N = \sum_{i=1}^c N_i$. Further, it is also assumed that $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N \in \mathcal{M}$ where \mathcal{M} in a non-linear manifold embedded in \mathbb{R}^d .

To reduce the dimensionality of images, He and Niyogi [11] have proposed an algorithm called Locality Preserving Projection (LPP). The outline of the algorithm is as follows:

Step 1: Construction of Adjacency Graph

Let the data samples $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_N$ represent the nodes of a graph G . Then, \mathbf{x}_i and \mathbf{x}_j are connected by an edge if they are close to each other depending upon any of the following criteria:

- (a) **ϵ -neighbourhood:** Here, two vectors \mathbf{x}_i and \mathbf{x}_j are said to be neighbours if $\|\mathbf{x}_i - \mathbf{x}_j\|^2 < \epsilon$ where norm is the Euclidean norm in \mathbb{R}^n .

(b) ***k* nearest neighbours**: Here, two vectors \mathbf{x}_i and \mathbf{x}_j are said to be neighbours if \mathbf{x}_i is among *k* nearest neighbours of \mathbf{x}_j or vice versa.

Step 2: Construction of Weight Matrix

Here, the weight matrix **S** is a sparse symmetric matrix of size $N \times N$ with S_{ij} as the weight joining the nodes \mathbf{x}_i and \mathbf{x}_j . There are two possible ways for defining S_{ij} i.e.

(a) **Heat Kernel**: If \mathbf{x}_i and \mathbf{x}_j are connected, put

$$S_{ij} = e^{-\frac{\|\mathbf{x}_i - \mathbf{x}_j\|^2}{\gamma}} \tag{1}$$

where $\gamma \in \mathbb{R}$ is a user defined parameter to control the weight values.

(b) **Simple Minded**: Here $S_{ij} = 1$ if \mathbf{x}_i and \mathbf{x}_j are neighbours and 0 otherwise.

Step 3 : Finding the Eigenmaps

The main objective of LPP is to find such a transformation **V** such that the connected points in the original space stay as close to each other as possible in the transformed space. Thus, LPP aims to minimize the following objective function:

$$\sum_{ij} (\mathbf{y}_i - \mathbf{y}_j)^2 S_{ij} \tag{2}$$

where \mathbf{y}_i is the representation of \mathbf{x}_i in the transformed space. Hence, the criterion function for LPP is given as follows [11]

$$J(\mathbf{V}_{LPP}) = \arg \min_{\mathbf{V}^T \mathbf{X} \mathbf{D} \mathbf{X}^T \mathbf{V} = \mathbf{I}} \mathbf{V}^T \mathbf{X} \mathbf{L} \mathbf{X}^T \mathbf{V} \tag{3}$$

where $\mathbf{X} = [\mathbf{x}_1 \ \mathbf{x}_2 \ \dots \ \mathbf{x}_N]$, **D** is a diagonal matrix with $D_{ii} = \sum_j W_{ij}$, representing the sum of weights in rows or columns. **L** = **D** – **W** is the Laplacian matrix.

The solution to the criteria in (3). Obtain the eigenvalue decomposition of the following generalized eigenvector problem:

$$\mathbf{X} \mathbf{L} \mathbf{X}^T \mathbf{v} = \lambda \mathbf{X} \mathbf{D} \mathbf{X}^T \mathbf{v} \tag{4}$$

Let the solution to the (4) is given by eigenvectors $\mathbf{v}_1, \mathbf{v}_2 \dots \mathbf{v}_l$ corresponding to the eigenvalues $\lambda_1 < \lambda_2 < \dots < \lambda_l$. Hence the original face images are represented in a lower dimensional embedding as follows:

$$\mathbf{x}_i \rightarrow \mathbf{y}_i = \mathbf{V}_{LPP}^T \mathbf{x}_i \quad \text{where} \quad \mathbf{V}_{LPP} = [\mathbf{v}_1, \mathbf{v}_2 \dots \mathbf{v}_l] \tag{5}$$

Now the transformed data points matrix **Y** is given by the following equation:

$$\mathbf{Y} = \mathbf{V}_{LPP}^T \mathbf{X} \tag{6}$$

Hence the dimensionality of the original data samples is reduced from \mathbb{R}^d to \mathbb{R}^l .

3 Proposed method

Cancelable biometric must possess two important criteria i.e. *viz.* non-invertible and revocable. In the proposed method, we find a low dimensional representation of the given training images using LPP [11]. This low dimensional representation corresponds to the coefficients corresponding the chosen eigenvectors and are non-invertible. Thus, instead of storing original biometric images, one can store the extracted features of an image. The second criterion of revocability is achieved by employing a random permutation matrix. A random permutation matrix is an identity matrix whose rows or columns are randomly exchanged in such a manner that each row and each column has only one entry as 1 while all others are 0.

Now, we see how revocable biometric pattern can be issued to an individual based on the proposed method.

3.1 Random permutation locality preserving projection (RP-LPP)

Since LPP [11] involves converting the biometric image to a column vector, in this proposed technique, the training images are pre multiplied with a random permutation matrix $\mathbf{P} \in \mathbb{R}^{d \times d}$ which permutes the original features of an identity. This process generates a *cryptic pattern* (where *pattern* \in {face, fingerprint, iris, voice etc.}) and is issued to the user. This biometric pattern is completely revocable and can be reissued if compromised. The cryptic pattern $\mathbf{z} \in \mathbb{R}^d$ corresponding to a biometric image $\mathbf{x} \in \mathbb{R}^d$ is computed using the following equation.

$$\mathbf{z} = \mathbf{P}\mathbf{x} \quad (7)$$

A sample face image and its corresponding cryptic face is shown in Fig. 1. The major contribution of our research work is the relationship between eigenvalues and eigenvectors of original biometric images and cryptic patterns. The eigenvalues possessed by the original biometric images and the cryptic pattern are same while the eigenvectors of the cryptic patterns are randomly permuted version of the eigenvectors of the original biometric images according to the random permutation matrix \mathbf{P} . The mathematical formulation of the relationship is given in the following subsection.



Fig. 1 Sample face Image (left) and its corresponding cryptic face (right) generated using RP-LPP

3.1.1 Theoretical analysis of relationship between IPP and RP-LPP

Suppose each of the training data vector \mathbf{x}_i ($i = 1, 2, \dots, N$) as given in Sect. 2 is permuted with the random permutation matrix \mathbf{P} so that the resulting training data after permutation is represented by \mathbf{z}_i as follows:

$$\mathbf{z}_i = \mathbf{P}\mathbf{x}_i \tag{8}$$

Hence, the criterion function of LPP as given in (2) is modified as follows:

$$\begin{aligned} V' &= \arg \min_{\mathbf{V}} \frac{1}{2} \sum_{ij} (\mathbf{y}_i - \mathbf{y}_j)^2 \mathbf{S}_{ij} \\ &= \frac{1}{2} \sum_{ij} (\mathbf{V}^T \mathbf{z}_i - \mathbf{V}^T \mathbf{z}_j)^2 S_{ij} \\ &= \frac{1}{2} \sum_{ij} (\mathbf{V}^T \mathbf{z}_i - \mathbf{V}^T \mathbf{z}_j)^T (\mathbf{V}^T \mathbf{z}_i - \mathbf{V}^T \mathbf{z}_j) S_{ij} \\ &= \frac{1}{2} \sum_{ij} (\mathbf{z}_i^T \mathbf{V} - \mathbf{z}_j^T \mathbf{V})(\mathbf{V}^T \mathbf{z}_i - \mathbf{V}^T \mathbf{z}_j) S_{ij} \\ &= \frac{1}{2} \sum_{ij} (\mathbf{V}^T \mathbf{z}_i S_{ij} \mathbf{z}_i^T \mathbf{V} - \mathbf{V}^T \mathbf{z}_i S_{ij} \mathbf{z}_j^T \mathbf{V} - \mathbf{V}^T \mathbf{z}_j S_{ij} \mathbf{z}_i^T \mathbf{V} + \mathbf{V}^T \mathbf{z}_j S_{ij} \mathbf{z}_j^T \mathbf{V}) \\ &= \frac{1}{2} \sum_{ij} (2\mathbf{V}^T \mathbf{z}_i S_{ij} \mathbf{z}_i^T \mathbf{V} - 2\mathbf{V}^T \mathbf{z}_i S_{ij} \mathbf{z}_j^T \mathbf{V}) \\ &= \sum_{ij} (\mathbf{V}^T \mathbf{z}_i S_{ij} \mathbf{z}_i^T \mathbf{V} - \mathbf{V}^T \mathbf{z}_i S_{ij} \mathbf{z}_j^T \mathbf{V}) \\ &= \sum_i \mathbf{V}^T \mathbf{z}_i M_{ii} \mathbf{z}_i^T \mathbf{V} - \sum_{ij} \mathbf{V}^T \mathbf{z}_i S_{ij} \mathbf{z}_j^T \mathbf{V} \\ &= \mathbf{V}^T \mathbf{Z} \mathbf{M} \mathbf{Z}^T \mathbf{V} - \mathbf{V}^T \mathbf{Z} \mathbf{S} \mathbf{Z}^T \mathbf{V} \\ &= \mathbf{V}^T \mathbf{Z} (\mathbf{M} - \mathbf{S}) \mathbf{Z}^T \mathbf{V} \\ &= \mathbf{V}^T \mathbf{Z} \mathbf{L} \mathbf{Z}^T \mathbf{V} \end{aligned}$$

where \mathbf{M} is a diagonal symmetric matrix and the entries at diagonals are row or column sums of \mathbf{S}_{ij} i.e. $M_{ii} = \sum_j S_{ij}$. The matrix $\mathbf{L} = \mathbf{M} - \mathbf{S}$ is the popular Laplacian matrix. The matrix \mathbf{M} gives information about the relative importance of the data points i.e. bigger the value of M_{ii} , more important is \mathbf{y}_i . Therefore, like [11], we also impose a constraint as follows:

$$\mathbf{Y}^T \mathbf{M} \mathbf{Y} = \mathbf{1} \implies \mathbf{V}^T \mathbf{Z} \mathbf{M} \mathbf{Z}^T \mathbf{V} = \mathbf{I} \tag{9}$$

Hence, the overall criterion of the proposed method becomes:

$$J(\mathbf{V}') = \arg \min_{\mathbf{V}^T \mathbf{Z} \mathbf{D} \mathbf{Z}^T \mathbf{V} = \mathbf{I}} \mathbf{V}^T \mathbf{Z} \mathbf{L} \mathbf{Z}^T \mathbf{V} \tag{10}$$

or

$$J(\mathbf{V}') = \arg \min_{\mathbf{V}^T \mathbf{P} \mathbf{X} \mathbf{D} \mathbf{X}^T \mathbf{P}^T \mathbf{V} = \mathbf{I}} \mathbf{V}^T \mathbf{P} \mathbf{X} \mathbf{L} \mathbf{X}^T \mathbf{P}^T \mathbf{V} \tag{11}$$

The above criterion is equivalent to (3) provided:

$$\mathbf{V}_{LPP} = \mathbf{P}^T \mathbf{V}' \tag{12}$$

This can be rewritten as:

$$\mathbf{V}' = \mathbf{P}\mathbf{V}_{LPP} \quad (13)$$

Thus, the transformation matrix \mathbf{V}' obtained after random permutation of the training images is simply the randomly permuted transformation matrix \mathbf{V}_{LPP} obtained with original training images.

3.1.2 Applicability of RP-LPP as cancelable biometric

From the above discussion, relationship between original and randomly permuted face images is revealed. But it is unacceptable to employ a single random permutation matrix \mathbf{P} for all the identities enrolled in the biometric recognition system. This will cause problems if the biometric template of any identity is compromised, then all the identities must be issued some new biometric template which is impractical. Thus to overcome this, each identity is issued a separate biometric template along with a key called personal identification number (PIN). When the user provides the cryptic pattern to the recognition system, he also presents the PIN issued to him during enrolment. This PIN determines the permutation matrix \mathbf{P}_i corresponding to that person and the appropriate transformation matrix \mathbf{V}'_i is obtained corresponding to that person as given below:

$$\mathbf{V}'_i = \mathbf{P}_i\mathbf{V}_{LPP} \quad (14)$$

First the biometric template is converted into a column vector and then the above transformation matrix directly converts the biometric template into feature vector without converting it to original face image. After obtaining the features, the identity of the person is determined by matching the features with the database. If either the biometric pattern or the PIN or both are not in order, then the user is rejected.

3.2 Applicability of RP-LPP in single sample scenario

The performance of the biometric recognition system depends on the number of training images available for training and it increases as more number of training images are available [18]. But due to the intricacies involved in collecting biometric samples in real life scenarios, it is presumed that the feature extraction method should perform well with small number of training images per identity. This leads to an interesting problem when only a single training image is available and this problem is known as one sample per person problem. A survey of one sample per person in the domain of face recognition is carried out by Tan et al. [43]. When only one sample is available, then several techniques as given in Kumar et al. [18] fail to work. However, the proposed method is applicable in such scenarios.

4 Experimental set-up

To demonstrate the effectiveness of the proposed techniques, we have performed experiments of three freely available datasets including face, iris and ear biometric. The details of the datasets is given in Table 1.

ORL [41] face dataset consists of facial images of 40 different identities with 10 images per person. The images of some identities were captured at different points of time with

Table 1 Summary of datasets used in experiments

Dataset	No. of identities	Original image size	Total images
ORL	40	112 × 92	400
UBIRIS	241	150 × 200	1877
IITD	125	180 × 50	493

varying illumination and facial expressions. These expressions include open or closed eyes, smiling or not smiling, or the face images have glasses / no glasses). The facial images in ORL dataset are gray level images with size of 112×92 pixels.

UBIRIS [37] is an iris database released by University of Beira, Portugal. It consists of 1877 gray scale images of 241 identities. These images are incorporated with several noise factors in order to evaluate the robustness of the algorithms. We have selected 5 images per person for experiments resulting into a total of 1205 images. These images are resized to half of the original size i.e. 75×100 .

IITD [17] is a database consisting of ear images of IIT Delhi students and staff members. The database was collected from people in the age group 14–58 years. The original database has 471 images of size 204×272 . The database also provides automatically segmented and cropped images of 125 people consisting of 493 ear images each of size 180×50 . We have selected 3 images of each person for our experiments resulting into a total of 375 images.

Sample images of one identity from each of the face, iris and ear datasets are shown in Fig. 2. The performance of the proposed techniques is evaluated in terms of the quality of the cancelable biometric template, security provided by cryptic patterns generated using RP-LPP, average classification accuracy and average training time of the algorithm. The training images from each identity is selected randomly and the remaining images are used as testing set. This process is repeated 40 times to achieve a stable classification accuracy and average training time. All the experiments are performed on Intel Xeon E3 CPU 2.4 GHz with Windows 8.1 and 16 GB main memory.

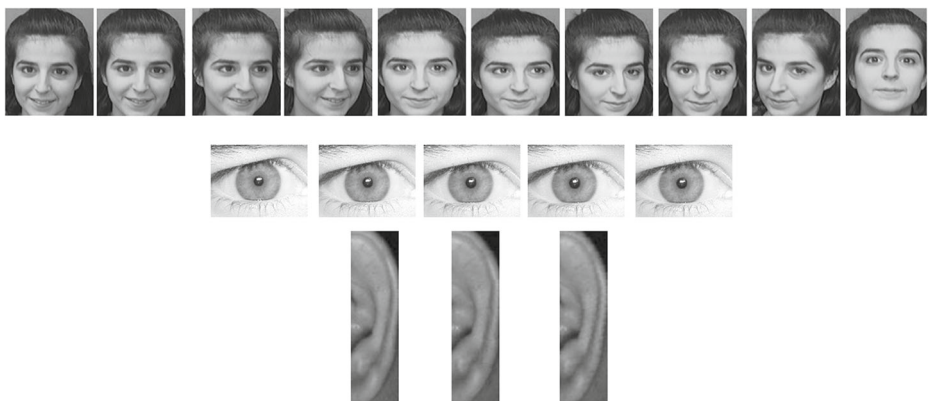


Fig. 2 Sample images of an identity from ORL [41] (top), UBIRIS [37] (middle) and IITD [17] (bottom) datasets

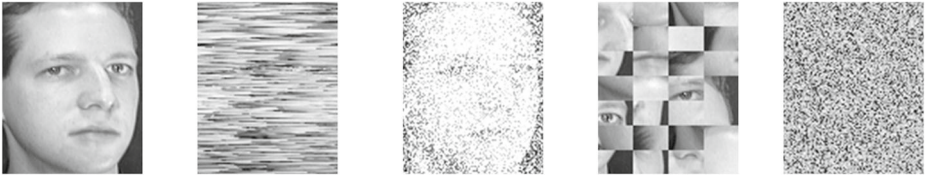


Fig. 3 Sample face images with corresponding cryptic patterns generated using Gray Combo, Gray Salt, Block Remapping and RP-LPP respectively(left to right) on ORL Face Dataset

5 Results and discussion

In this section, we critically analyse the performance of the proposed method i.e. RP-LPP both qualitatively and quantitatively with other state-of-the-art methods viz. GRAY-COMBO (GC), GRAY-SALT(GS) and BLOCK-REMAPPING(BR). We have obtained the cryptic pattern using the compared methods and then features are extracted using LPP. Finally, recognition is performed using Nearest Neighbour (NN) rule. The performance of the proposed methods is analysed using security of biometric template generated using the proposed techniques against the brute force attack. The quality of cryptic patterns generated by the proposed methods is also compared with the above-mentioned methods. Further, we present and discuss average classification accuracy and compare it with state-of-the-art methods. The average training time required by the proposed techniques is also shown. RP-LPP is trained using only few training images from each identity so as to tackle SSS problem.

5.1 Analysis of cryptic patterns

5.1.1 Security against brute force attack

Here, we analyse the cryptic patterns or biometric templates produced using the proposed RP-LPP method both qualitatively and quantitatively. Some examples face, iris and ear images with their corresponding biometric templates produced using GRAY-COMBO (GC), GRAY-SALT (GS), Block-Remapping (BR) and the proposed RP-LPP are shown in Figs. 3, 4 and 5 respectively. It is apparent from these figures that the quality of cryptic patterns generated using the proposed Random Permutations is better in comparison to all other compared methods. It is also observed that the cryptic pattern generated by other methods (GC,GS,BR) leave some information which can be exploited to know the original biometric pattern and thus are vulnerable. However, the cryptic patterns generated using the proposed techniques leave no room for such kind of guessing. It can be further observed from Figs. 3, 4 and 5 that there is no pattern whatsoever when biometric template is generated

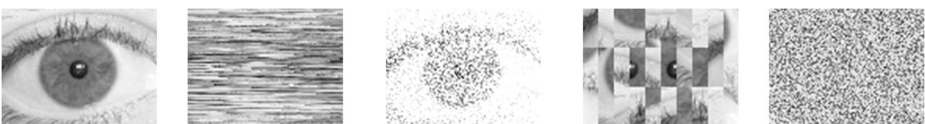


Fig. 4 Sample iris images with corresponding cryptic patterns generated using Gray Combo, Gray Salt, Block Remapping, RP-LPP respectively(left to right) on UBIRIS Iris Dataset

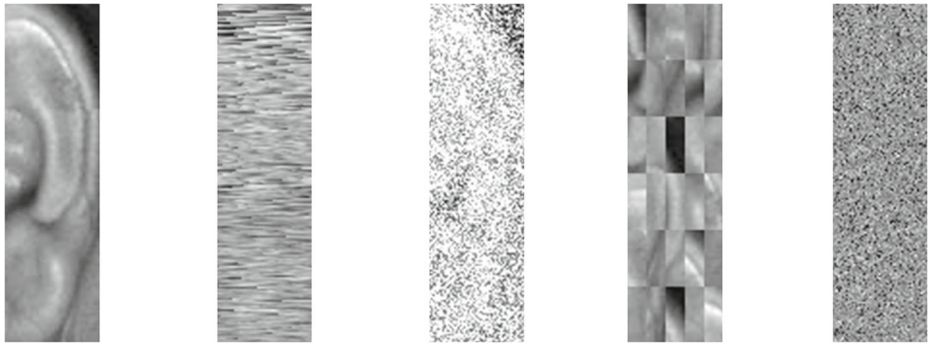


Fig. 5 Sample ear images with corresponding cryptic patterns generated using Gray Combo, Gray Salt, Block Remapping, RP-LPP respectively(left to right) on IIT Delhi Ear Dataset

using RP-LPP and biometric templates generated from the proposed method is completely revocable and can be reissued if compromised.

As biometric template generated using the proposed techniques is a random permutation of the features of original biometric template, the robustness of the biometric template can be estimated from the image size say $d = a \times b$. As in RP-LPP, each biometric image is represented as a column vector, the brute force attack requires $d!$ iterations (where $d = a \times b$) which is extremely hard to break in practice. For a typical biometric template of size 100×100 , the number of possible iterations shall be of the order of 10000! which is a very large number. In addition to this, the PIN which is issued to the identity further makes it harder to break the encryption.

Let us suppose that we have fastest supercomputer at our disposal with a speed of 100 Peta FLOPS $\approx 10^{17}$ floating point operations per second and assume that matrix multiplication requires 1 basic step. Then it requires $(a \times b)!$ iterations for the random permutation matrix in case of RP-LPP. Furthermore, random permutation matrix multiplication with the image converted to column vector requires d^2 multiplications where $d = a \times b$ in RP-LPP. We know that there are 86400 sec. ($= 24 \times 60 \times 60$) in a day. The time required to brute force the cryptic patterns generated using the proposed techniques is given in Table 2. It can be easily observed from the Table that it will take several centuries to break the cryptic pattern using brute force attack thereby ensuring the high security of the biometric template. The least time to break the biometric template is for UBIRIS iris dataset when RP-LPP is employed for generating the biometric template. But, it still requires 10^{25792} years which is very high. Hence, the proposed techniques generate highly secure biometric patterns.

Table 2 Time required to break the cryptic pattern of brute force attack

Dataset	# Iterations for brute force	Time required for brute force attack (years)
ORL	$10304! \approx 10^{36878}$	$\frac{10^{36878} \times (10304)^2}{10^{17} \times 86400 \times 365} \approx 10^{36871}$
UBIRIS	$7500! \approx 10^{25809}$	$\frac{10^{25809} \times (7500)^2}{10^{17} \times 86400 \times 365} \approx 10^{25792}$
IITD	$9000! \approx 10^{31682}$	$\frac{10^{31682} \times (9000)^2}{10^{17} \times 86400 \times 365} \approx 10^{31665}$

5.1.2 Non-invertibility of generated templates

One of the essential requirement of cancelable biometric template is that it is non-invertible. In the proposed approach, the generated template and the PIN is provided by the user to the system for authentication. This information is used to determine the permutation matrix and hence extract the features which are used for authentication without any control of the user. This information is further used to extract the distinguishing few features (typically 20 as shown in experimental results) out of a large number of features as discussed. Reconstruction of the biometric image using these 20 features is very hard. Even if an intruder gets access to these 20 features, then reconstruction shall result in cancelable biometric image which is extremely difficult to decode in limited time. This proves that the generated templates using the proposed method are non-invertible.

5.1.3 Correlation analysis

Here, we analyse the correlation between generated templates by changing the random permutation matrix \mathbf{P} . The analysis is similar to [15]. The transformed templates are diverse if the correlation between any two generated templates is low and is computed as :




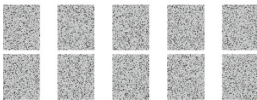
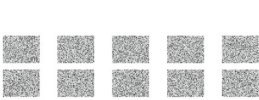
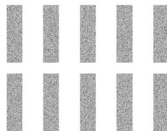
$$R = \frac{\sum(T_1 - \bar{T}_1)(T_2 - \bar{T}_2)}{\sqrt{(T_1 - \bar{T}_1)^2 + (T_2 - \bar{T}_2)^2}} \tag{15}$$

where T_1 and T_2 are the generated templates with \bar{T}_1 and \bar{T}_2 representing the mean template values respectively. We have chosen a sample image from each of the datasets as shown in Table 3. Then 10 different templates are generated by changing the random permutation matrix. For each pair of the generated templates, correlation coefficient is determined using above equation and average of the absolute value of correlation is reported in the last row of the Table 3. It can be readily observed that the average absolute correlation is less than 2% across all the datasets which clearly indicates that no mutual information is available between any two generated templates. This average value is also known as Correlation Index(CI) of the dataset. The proposed method is able to achieve good CI on all the datasets.

5.2 Classification accuracy

The classification accuracy measures the percentage of identities correctly classified by some technique or algorithm. This classification accuracy of a technique depends on factors such as the number of training images used, the number of dimensions in the transformed

Table 3 Average absolute correlation index

Dataset	ORL	UBIRIS	IITD
Sample image			
Generated templates			
Correlation index	1.42%	1.91%	1.46%

representation. The technique which gives better performance with few number of training images is of real significance. In our experiments, we have kept the number of training images less than 6 and the number of reduced dimension only upto 20. These can be modified according to the application at hand. We have measured the classification accuracy of the proposed techniques on ORL, UBIRIS and IITD datasets and is shown in Figs. 6, 7 and 8 respectively. This average classification accuracy is obtained after 40 random runs as explained in previous section. In the rest of this section classification accuracy means average classification accuracy unless otherwise stated.

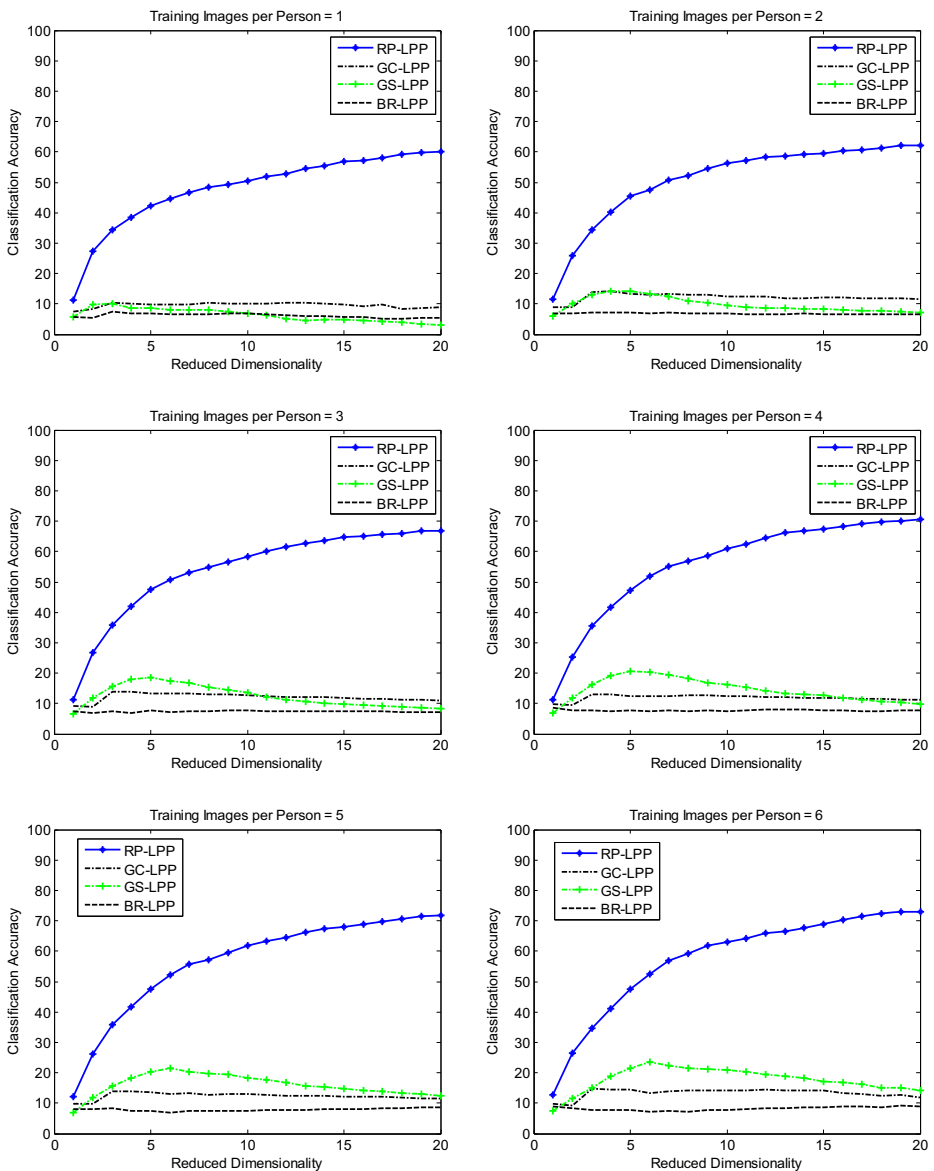


Fig. 6 Classification Accuracy on ORL face dataset

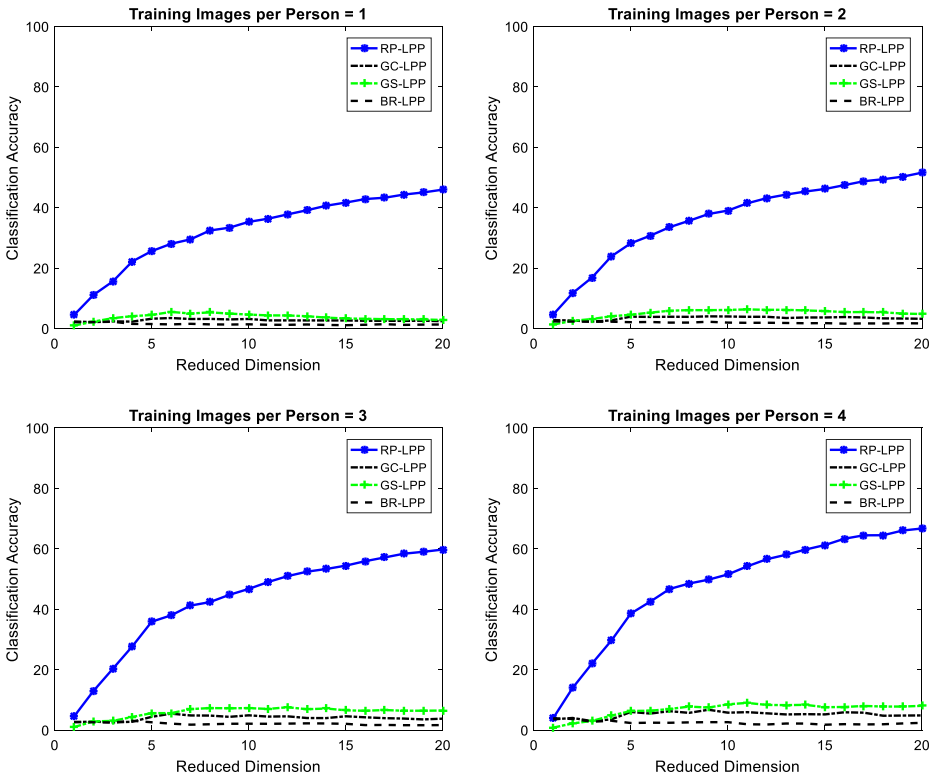


Fig. 7 Classification Accuracy on Ubiiris iris dataset

The training images for each identity in ORL [41] face dataset are varied from 1 to 6. The classification for each case is shown in Fig. 6. It can be easily observed that the classification accuracy for RP-LPP is better than all other compared methods. It is interesting to note that the classification accuracy of RP-LPP is more than 60% when a single training images per identity is used. This classification accuracy further increases to more than 70% with 6

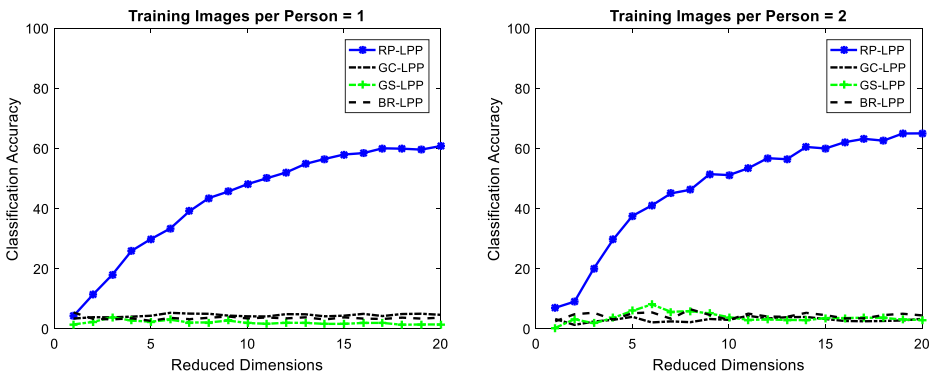


Fig. 8 Classification Accuracy on IITD ear dataset

training images. Also, the classification accuracy of other methods is less than 25% across all the scenarios considered here.

For experiments on UBIRIS [37] iris dataset, the training images are varied from 1 to 4 as shown in Fig. 7. RP-LPP outperforms all other methods in all cases. The increases in classification accuracy is almost linear with the number of reduced dimension. It can be noticed that with a single training image, RP-LPP achieves a classification accuracy of approximately 50% which increases to almost 70% when the number of training images increase to 4.

The classification accuracy on IITD [17] ear dataset is shown in Fig. 8. As only few training images are available in the dataset, we could use only 1 or 2 images of each identity as the training images. However, the classification accuracy of the proposed techniques is encouraging and similar observations as that on ORL and UBIRIS are observed on this dataset also. A classification accuracy of 65% is achieved by RP-LPP when 2 training images are used. The proposed techniques perform better than other methods. At some places, the classification accuracy slightly decreases at few places. Thus, we can say that the increase in number of reduced dimensions does not guarantee an increase in the classification accuracy. But the classification accuracy generally increases with increase in the number of reduced dimension. On all the datasets, RP-LPP performs best in all cases.

5.3 Training time

The average training time of proposed method RP-LPP and other compared methods on all the datasets as shown in Table 4. It can be readily observed that the training time of the

Table 4 Training time (sec.) required by proposed method on ORL, UBIRIS and IITD dataset

Dataset	ORL					
Training Images/Person	1	2	3	4	5	6
RP-LPP	0.0133	0.0269	0.0451	0.0626	0.0865	0.1096
GC-LPP	0.0135	0.0297	0.0455	0.0649	0.0937	0.1194
GS-LPP	0.0102	0.0272	0.0481	0.0646	0.0887	0.1172
BR-LPP	0.0100	0.0279	0.0453	0.0631	0.0832	0.1120
Dataset	UBIRIS					
Training Images/Person	1	2	3	4		
RP-LPP	0.0862	0.2423	0.4591	0.7026		
GC-LPP	0.0959	0.2780	0.5440	0.8890		
GS-LPP	0.0912	0.2899	0.5949	0.9688		
BR-LPP	0.0870	0.2438	0.4615	0.7816		
Dataset	IITD					
Training Images/Person	1	2				
RP-LPP	0.0388	0.0892				
GC-LPP	0.0433	0.1137				
GS-LPP	0.0440	0.1086				
BR-LPP	0.0416	0.0972				

The bold values indicate the minimum training time among the compared methods

proposed method is less in comparison to other methods on all the datasets except two cases on ORL dataset (where no. of training image(s) are 1 and 5). Further, it is also noticed that the training time of various techniques increases with increase in number of training images. This comparison also supports the superiority of the proposed method.

6 Conclusion

In this paper, we presented a simple and powerful techniques based on random permutations. The proposed techniques RP-LPP is applicable to cancelable biometric recognition in which the identities are issued a biometric template which we call cryptic pattern based on random permutation matrices along with a PIN. The identities present both the cryptic pattern and the PIN in order to be recognized by the system. If any of the two is incorrect, then the identity is rejected by the system. Experimental results demonstrate the effectiveness of the proposed techniques. The cryptic pattern generated by RP-LPP is highly secure and it will take centuries to break the code using brute force attack. Even if the biometric template is compromised, the same can be reissued. The proposed technique is also applicable to scenarios where only single sample per person is available for training. Another key advantage of the proposed method is that no image registration is required during enrolment. The performance of the proposed techniques are measured on three freely available face, iris and ear datasets against other random permutation methods. The performance was found to be better in terms of quality and security of cryptic patterns, average classification accuracy and average training time. RP-LPP outperforms other methods in terms of classification accuracy and training time. Further, experimental results demonstrate the robustness of the proposed techniques across different biometrics.

References

1. Al-juboori AM, Bu W, Wu X, Zhao Q (2014) Palm vein verification using multiple features and locality preserving projections. *The Scientific World Journal*, 2014, Article ID 246083, 11 pages
2. Bellman RE (1961) *Adaptive control processes*. Princeton University Press, Princeton
3. Bolle RM, Connel JH, Ratha NK (2002) Biometrics perils and patches. *Pattern Recogn* 35(12):2727–2738
4. Cox TF, Cox MA (2001) *Multidimensional scaling*. CRC Press, Boca Raton
5. Cunningham JP, Ghahramani Z (2015) Linear dimensionality reduction: survey, insights, and generalizations. *J Mach Learn Res* 16:2859–2900
6. Douchamps D, Campbell N (2007) Robust real time face tracking for the analysis of human behaviour. In: *Proceedings of the 4th international conference on machine learning for Multimodal Interaction*, Berlin, Heidelberg, pp 1–10
7. Fisher RA (1936) The use of multiple measurements in taxonomic problems. *Annals of Eugenics* 7(2):179–188
8. Gao Q, Zhang C (2017) Constructing cancellable template with synthetic minutiae. *IET Biometrics* 6(6):448–456
9. Gong Y (1995) Speech recognition in noisy environments: a survey. *Speech Comm* 16(3):261–291
10. Hammerle-Uhl J, Pschernig E, Uhl A, Samarati P, Yung M, Martinelli F, Ardagna CA (2009) Cancelable iris biometrics using block re-mapping and image warping. In: *Proc. of the 12th international conference on information security*, Pisa, Italy, pp 135–142
11. He X, Niyogi P (2004) Locality preserving projections. In: *Advances in neural information processing systems*, p 16
12. Hotelling H (1936) Relations between two sets of variates. *Biometrika* 28:321–377
13. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. *IEEE Trans Circ Syst Video Technol* 14(1):4–20

14. Jin Z, Hwang JY, Lai Y, Kim S, Teoh ABJ (2018) Ranking-based locality sensitive hashing-enabled cancelable biometrics: index-of-max hashing. *IEEE Trans Inform Forensics Secur* 13(2):393–407
15. Kaur H, Khanna P (2017) Non-invertible biometric encryption to generate cancelable biometric templates. In: Proc. of the world congress on engineering and computer science (WCECS 2017), USA
16. Kaur H, Khanna P (2019) Random distance method for generating unimodal and multimodal cancelable biometric features. *IEEE Trans Inform Forensics Secur* 14(3):709–719
17. Kumar A, Wu C (2012) Automated human identification using ear imaging. *Pattern Recogn* 41(5):956–968
18. Kumar N, Jaiswal A, Agrawal RK (2012) 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 '12), ACM, New York, NY, USA, pp 938–944
19. Lee DH, Lee S, Ik Cho N (2018) Cancelable biometrics using noise embedding. In: Proc. of the 24th international conference on pattern recognition (ICPR), pp 3390–3395
20. Leng L, Li M, Leng L, Teoh ABJ (2013) Conjugate 2DPalmhash code for secure palm-print-vein verification. In: Proc. of the 6th international congress on image and signal processing (CISP), Hangzhou, pp 1705–1710
21. Leng L, Teoh ABJ (2015) Alignment-free row-co-occurrence cancelable palmprint. *Fuzzy Vault Pattern Recogn* 48(7):2290–2303. <https://doi.org/10.1016/j.patcog.2015.01.021>
22. Leng L, Teoh AB, Li M (2017) Simplified 2DPalmHash code for secure palmprint verification. *Multimed Tools Appl* 76(6):8373–8398. <https://doi.org/10.1007/s11042-016-3458-3>
23. Leng L, Zhang J (2013) PalmHash Code vs. PalmPhasor Code. *Neurocomputing* 108:1–12. <https://doi.org/10.1016/j.neucom.2012.08.028>
24. Leng L, Zhang J, Xu J, Khan K, Alghathbar K (2010) Dynamic weighted discrimination power analysis: a novel approach for face and palmprint recognition in DCT domain. *Int J Phys Sci* 5:467–471
25. Leng L, Zhang J, Xu J, Khan MK, Alghathbar K (2010) Dynamic weighted discrimination power analysis in DCT domain for face and palmprint recognition. In: Proc. of international conference on information and communication technology convergence (ICTC), Jeju, 2010, pp 467–471
26. Leng L, Zhang J, Chen G, Khan MK, Alghathbar K (2011) Two-directional two-dimensional random projection and its variations for face and palmprint recognition. In: Murgante B, Gervasi O, Iglesias A, Taniar D, Apduhan BO (eds) Computational science and its applications - ICCSA 2011. Springer, Berlin, pp 458–470
27. Leng L, Zhang J, Chen G, Khan MK, Bai P (2011) Two dimensional palmphasor enhanced by multi-orientation score level fusion. In: Park JJ, Lopez J, Yeo SS, Shon T, Taniar D (eds) Secure and trust computing, data management and applications. Springer, Berlin, pp 122–129
28. Leng L, Zhang JS (2012) Palmhash code for palmprint verification and protection. Proc. of 25th IEEE Canadian Conf. Electr. Comp. Eng.: 1–4
29. Leng L, Zhang S, Bi X, Khan MK (2012) Two-dimensional cancelable biometric scheme. In: Proc. of the international conference on wavelet analysis and pattern recognition, Xian, pp 164–169
30. Maiorana E, Campisi P, Fierrez J, Ortega-García J, Neri A (2010) Cancelable templates for sequence-based biometrics with application to on-line signature recognition. *IEEE Trans Syst Man Cybern A* 40(3):525–538
31. Marsico MD, Petrosino A, Ricciardi S (2016) Iris recognition through machine learning techniques: a survey. *Pattern Recognition Letters*, Available online
32. Patel VM, Ratha NK, Chellappa R (2015) Cancelable Biometrics: a review. *IEEE Signal Processing Magazine* 32(5):54–65
33. Pearson K (1901) On lines and planes of closest fit to systems of points in space. *Phil Mag* 2:559–572
34. Peralta D, Galar M, Triguero I, Paternain D, García S, Barrenechea E, Benítez JM, Bustince H, Herrera F (2015) A survey on fingerprint minutiae-based local matching for verification and identification: taxonomy and experimental evaluation. *Inform Sci* 315(10):67–87
35. Pillai JK, Patel VM, Chellappa R, Ratha NK (2011) Secure and robust iris recognition using random projections and sparse representations. *IEEE Trans Pattern Anal Mach Intell* 30(9):1877–1893
36. Prabhakar S, Pankanti S, Jain AK (2003) Biometric recognition: security and privacy concerns. *IEEE Security Privacy Mag* 1(2):33–42
37. Proença H, Alexandre LA (2005) UBIRIS: a noisy iris image database, 13th International Conference on Image Analysis and Processing - ICIAP 2005, Springer, vol. LNCS 3617, 970–977
38. Ratha N, Chikkerur S, Connell J, Bolle R (2007) Generating cancelable fingerprint templates. *IEEE Trans Pattern Anal Mach Intell* 29(4):561–572
39. Ratha NK, Connell JH, Bolle R (2001) Enhancing security and privacy in biometrics- based authentication systems. *IBM Syst J* 40(3):614–634

40. Rathgeb C, Breiting F, Busch C, Baier H (2014) On the application of bloom filters to iris biometrics. *IET J Biometrics* 3(4):207–218
41. Samaria F, Harter A (1994) Parameterisation of a stochastic model for human face identification. In: *Proceedings of 2nd IEEE workshop on applications of computer vision, Sarasota FL*
42. Savvides M, Kumar B, Khosla P (2004) Cancelable biometric filters for face recognition. *Proc Int Conf Pattern Recognition* 3:922–925
43. Tan X, Chen S, Zhou ZH, Zhang F (2006) Face recognition from a single image per person: a survey. *Pattern Recogn* 39(9):1725–1745
44. Teoh A, Goh A, Ngo D (2006) 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
45. Turk M, Pentland A (1991) Eigenfaces for recognition. *J Cognitive Neuroscience* 3(1):71–86
46. Wiskott L (2003) Slow feature analysis: a theoretical analysis of optimal free responses. *Neural Comput* 15(9):2147–2177
47. Wiskott L, Sejnowski T (2002) Slow feature analysis: unsupervised learning of invariances. *Neural Comput* 14(4):715–770
48. Wu S, Chen P, Swindlehurst AL, Hung P (2019) Cancelable biometric recognition with ECGs: subspace-based approaches. *IEEE Trans Inform Forensics Secur* 14(5):1323–1336
49. Xu W, He Q, Li Y, Li T (2008) Cancelable voiceprint templates based on knowledge signatures. *Proc Int Symp Electronic Commerce and Security*: 412–415
50. Zhao W, Chellappa R, Phillips PJ, Rosenfeld A (2003) Face recognition: a literature survey. *ACM Comput Surv* 35(4):399–458
51. Zuo J, Ratha N, Connell J (2008) Cancelable iris biometric. *Proc Int Conf Pattern Recognition*: 1–4

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



Nitin Kumar received his Doctor of Philosophy and Master of Technology from School of Computer and System Sciences, Jawaharlal Nehru University, New Delhi. He is currently working as Assistant Professor in the Department of Computer Science and Engineering at National Institute of Technology, Uttarakhand, India. His current research include visual attention modeling, pattern recognition, face recognition and image processing.



Manisha Rawat received her M. Sc. in Computer Science from Kurukshetra University, Kurukshetra. Currently, she is pursuing her Doctor of Philosophy in Computer Science and Engineering at National Institute of Technology, Uttarakhand. His current research interests include Cancelable Biometrics, Pattern Recognition and Image Processing.