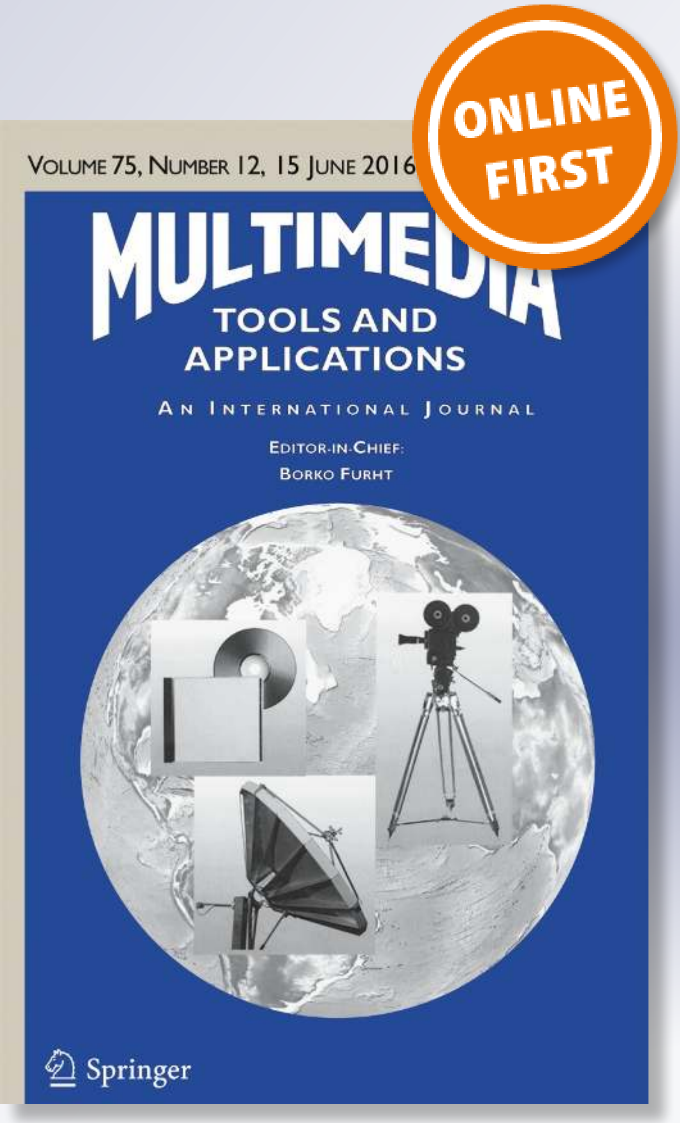
Cancelable features using log-Gabor filters for biometric authentication

Harkeerat Kaur & Pritee Khanna

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501

Multimed Tools Appl
DOI 10.1007/s11042-016-3652-3



Springer

Multimed Tools Appl
DOI 10.1007/s11042-016-3652-3

Cancelable features using log-Gabor filters for biometric authentication

Harkeerat Kaur[1] · Pritee Khanna[1]

Received: 2 November 2015 / Revised: 30 March 2016 / Accepted: 1 June 2016

Abstract Wide spread use of biometric based authentication requires security of biometric data against identity thefts. Cancelable biometrics is a recent approach to address the concerns regarding privacy of biometric data, public confidence, and acceptance of biometric systems. This work proposes a template protection approach which generates revocable binary features from phase and magnitude patterns of log-Gabor filters. Multi-level transformations are applied at signal and feature level to distort the biometric data using user specific tokenized variables which are observed to provide better performance and security against information leakage under correlation attacks. A thorough analysis is performed to study the performance, non-invertibility, and changeability of the proposed approach under stolen token scenario on multiple biometric modalities. It is revealed that generated templates are non-invertible, easy to revoke, and also deliver good performance.

Keywords Cancelable biometrics · Biometric salting · Log-Gabor transform · Non-invertiblity · Random projection · Revocability

1 Introduction

Biometric traits offer significant and highly sensitive information about an individual. While the use of biometric templates is easy, convenient and reliable, there are some security and privacy related issues that need to be addressed. Ratha et al. [49] identified eight points at which a generic biometric system can be attacked. Amongst many identified issues, stolen

✉ Pritee Khanna
pkhanna@iiitdmj.ac.in

Harkeerat Kaur
harkeerat.kaur@iiitdmj.ac.in

[1] Computer Science and Engineering, PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur, Madhya Pradesh, India

Published online: 05 July 2016

biometric scenario where an imposter is able to spoof by providing a stolen biometric sample of the genuine user is the current threat to deal with. Database attacks lead to permanent template compromise, where an attacker uses the stored biometric data to obtain illegitimate access. As biometric data is being increasingly shared among various applications, it also lead to tracing and tracking of users across different databases by matching their reference templates. Unlike passwords or PINs, biometric templates cannot be revoked on theft. Biometric templates are permanently associated with a particular individual and once compromised, they are lost forever. Moreover, the same template is stored across different application databases which can be compromised by cross-matching attack.

Cancelable biometrics suggests to use transformed version of the biometric data or extracted features for storing and matching purposes. Hence, in case of any attack, the compromised template can be revoked and new transformed versions can be generated by changing the transformation parameters. The objective of this work is to generate biometric templates which can be cancelled like passwords. The cancelability allows regeneration of biometric data in case of compromise and addresses above mentioned issues. The work proposes a multi-level transformation of biometric template using random projection and log-Gabor filters to generate cancelable feature vectors that can be efficiently used for biometric authentication without compromising on performance. Gabor and log-Gabor filters have been widely used for processing the biometric signal for robust extraction of feature vectors. The proposed approach extracts log-Gabor magnitude and phase patterns of biometric signal and salts them in a non-invertible fashion to generate transformed feature vectors which are binary strings. Experiments are performed to evaluate revocability and matching performance of the system under stolen token scenario and results reveal comparable performance with other non-revocable log-Gabor based feature extraction techniques. The applicability of the proposed approach is also tested on various biometric modalities such as visible and infrared faces, palmprints, palmveins, and fingerveins.

The work is organized as follows. Biometric template protection using cancelable biometrics with a literature review and rationale behind the work is provided in Section 2. Section 3 discusses some preliminaries followed by the proposed approach presented in Section 4. The experimental results and analysis is reported in Section 5 and the work is finally concluded in Section 6.

2 Template protection and cancelable biometrics

Template protection techniques suggest use of some auxiliary/helper data to transform the reference biometric into a new format such that the above mentioned concerns can be addressed. It is required that these transformed templates must not compromise the ability to identify/verify individuals, maintain discriminability and intra-user variability, and address various attack scenarios. Biometric template protection approaches can be broadly classified as – *Biometric Cryptosystems* and *Cancelable Biometrics*.

Biometric Cryptosystems combine the strength of biometrics and cryptography to get benefit from both sides. Cryptosystems utilize the extracted biometric features either to secure a cryptography key or to generate one from them. Although mainly designed to secure cryptographic keys, cryptosystems can also be used for template protection. Depending upon the coupling level of cryptography and biometrics, further classification is done into key-binding and key-generation schemes. Biometrics-based key binding schemes use biometric authentication to release a previously stored cryptographic key, whereas key generation schemes generate cryptographic key from biometric templates [51, 58].

Cancelable biometrics is a transformation based template protection approach that allows generation of revocable biometric templates which can be revoked like passwords innumerable times. Cancelable biometrics can be formally defined as "an intentional and systematically repeated distortions on the biometric data in order to protect the user sensitive information" [26]. A cancelable template is generated from biometric data by subjecting it to systematic distortions based on some transformation functions and user specific auxiliary data. Instead of the original biometric, the transformed template is used for storing and matching, while user specific auxiliary data is provided to the enrollee in a tokenized format. Cancelability can be achieved by distorting the template either at signal level or feature level [49]. At signal level the distortions are performed directly on the data collected at the sensors, whereas at feature level the extracted feature set is targeted. The main objectives of template protection using cancelable biometric template scheme are *Revocability*, *Diversity*, *Non-invertibility*, and *Performance* [26].

2.1 Literature review

Many simple techniques like grid morphing and block permutations are applied to distort the original biometric at signal level [6]. However, in literature most of the proposed approaches focus at feature level transformation. These approaches can be broadly classified as *biometric salting* and *non-invertible transformations*.

Biometric salting works on the same principle of salting as in cryptography, but for transforming biometric templates. Biometric salting blends independent input factor and user specific secret key (such as random numbers or passwords) with the biometric data and with the help of some transformations produces distorted templates. Secret key is generated externally and combined with the biometric data to increase entropy of the template, thus making it difficult for an adversary to make a guess. In case of a compromise, it is easy to revoke and generate a new template by changing key. Since the transformations are invertible, accuracy and vulnerability of the scheme depends upon the confidentiality of key.

BioHashing proposed by Teoh et al. is an instance of biometric salting in which a Tokenized (pseudo) Random Number (TRN) is combined with biometric features to generate BioCodes [24]. BioHashing has been experimentally reported to achieve nearly zero Equal Error Rates (ERR) for various modalities [13, 24, 55]. This substantial increase in performance is due to increase in inter-user variations caused by random projection. If BioCode and TRN are compromised, then BioHashing is invertible and pre-image attack can be performed to approximate original biometric [28, 30].

Savvides et al. proposed biometric salting for generating cancelable face templates using Minimum Average Correlation Energy (MACE) filter and random kernels [50]. However, its security may be jeopardized via deterministic de-convolution with a known random kernel. To enhance security features of this method, application of number theoretic transform on the biometric data before convolution with random kernels is proposed by Hirata and Takahashi [21]. Sutcu et al. proposed robust hashing technique for face templates which uses non-linear operations to achieve improved security [54]. A tradeoff is observed to get discriminability and non-invertibility.

Teoh et al. proposed BioPhasoring to generate cancelable fingerprints based on multichannel Gabor filter to address the invertibility issue [56]. The technique generates a set of complex vectors where the original vectors form the real part and rows of the orthonormal random vector form the imaginary part. This way BioPhasoring keeps on mixing user specified TRN with the biometric data iteratively to generate non-invertible templates and a straight forward revocation is possible by token replacement.

Recently, various Gabor filters based feature extraction and distortion techniques have been proposed to generate cancelable palmprints. Leng and Zhang used BioPhasoring and BioHashing to generate highly secure one dimensional and two dimensional PalmPhasor and PalmHash codes both relying on Gabor based feature extraction technique [32, 33]. They also employed 2D PalmPhasor codes to develop a dual-key-binding cancelable palmprint cryptosystem to overcome the lack of cancelability in existing biometric cryptosystems [32]. Leng et al. determined that 2D PalmHash Code are susceptible to statistical analysis attack due to vertical correlation and defined a suitable orientation range of Gabor feature matrices to prevent the same [36]. Recently, 2D PalmHash Code are combined with fuzzy vault primitive to protect palmprint templates [31]. A multimodal cancelable system which fuses 2D PalmHash Codes obtained from palmprint and palmvein biometrics to offers better recognition rates and verification accuracy is proposed in [35]. Leng et al. generated cancelable PalmCode from texture features obtained by randomized Gabor filters [34]. The parameters are randomized by the user-specific tokenized pseudo-random number (PRN) to generate filters that are used for feature extraction. However, the key space of chosen parameters is limited and very random values damage the extracted features.

Non-invertible transformation functions are one way surjective functions that are easy to compute but hard to inverse. Similar to salting techniques, a user specific key/token is associated with the transformation function during enrollment. In case template is compromised, a new one can be generated by simply changing the token or even the transformation function itself.

Non-invertible functions reported by Ratha et al. transformed fingerprint data by Cartesian, polar, or surface folding transformation on the minutiae positions [48]. Inspite of the claim of non-invertibility, successful attacks on approximating the original data from the transformed ones are presented in [47].

Farooq et al. presented a concept of generating cancelable bit strings from fingerprint by extracting translational and rotational invariant minutiae triplets [15]. On the same line, Lee et al. proposed minutiae based bit strings to generate cancelable fingerprint templates [29]. Minutiae are mapped onto a predefined 3-D array and bit strings are generated by assigning 1 to the cells containing more than one minutia points or 0 otherwise. These 1-D bit strings are subjected to some random permutation determined by user specific PIN. To achieve non-invertibility, transformation functions follow many to one mapping which may lead to distortions to an extent that the discriminability of the system may be compromised. Yang et al. generated cancelable fingerprint templates by applying non-invertible transforms to Delaunay triangle based local structure of minutiae points rather than individual minutiae points [63]. The method achieves good local structural stability even after distortion and efficiently preserves the discriminability capability of the transformed template without compromising on non-invertibility. These techniques mainly focus on fingerprints features which is represented as set of unordered minutiae positions. However, implementation of these techniques is not clear to other biometric modalities such as face, palmprints and iris where features representations are quite different from those of fingerprints.

Boult et al. proposed Biotokens, a cryptographically secure technique for face templates, which divides the datum into two parts. One part is used for encoding purpose and the other for approximating a match and support robust distance computation [7]. But if private key and transform parameters are known, the biometric features are recoverable. Maiorana et al.

proposed BioConvolving, a convolution based transformation for cancelable signature templates [42]. The template is expressed as a set of discrete finite sequences, which are divided into a fixed number of segments according to some randomly selected decomposition key. The transformation function is obtained by performing a linear convolution between segments. However, if the convolution kernel and key are known to an attacker, then the original signature signal may be approximated by attempting deconvolution.

2.2 Motivation behind the proposed work

The following observations are made from the literature review:

1. Biometric salting techniques increase performance of the system, but most of them are invertible.
2. Performance of many salting techniques are evaluated and reported in the best scenario assuming that the user specific token is not known to the attacker. However, the performance should be reported assuming the worst scenario when an attacker is always in possession of genuine users tokens.
3. Application of cancelable techniques is typically shown on a specific modality, e.g., fingerprint, face, palmprint or palmvein. A generic approach suitable for more and more modalities needs to be defined.
4. Most of the existing approaches distort biometric data at feature level as compared to signal level. In either way, there is always some mutual information content between transformed templates of the same user. This information leakage must be minimized to generate diverse templates.

This motivated us to develop a new salting technique that generates revocable and non-invertible biometric templates and performs well in stolen-token scenario. The transformations should preserve the discriminability of features so that the recognition accuracy of the system is maintained when it operates in transformed domain. Also, it should provide high level security at the same time. We studied the effects when distortion is applied at both the levels and observed that higher security against information leakage and correlation attacks is achieved with multi-level transformations as compared to single level transformations. This helps in determining the usability of particular biometric trait and practical number of times it can be revoked without giving up the confidentiality. This lead us to develop a multi-level transformation of biometric template using random projection and log-Gabor filters to generate cancelable features and check its applicability on various biometric modalities. In addition to minimizing correlation between transformed templates, random projection at signal level does significant dimension reduction. Use of random projection is especially useful when approaches like Gabor filters are used which output vectors at various scales and orientations. Also, if the sensor and feature extractor are not integrated at the same physical location, signal level distortions can help to enhance the security of data in transmission.

3 Preliminaries

The proposed approach is based on log-Gabor transform of randomly projected biometric sample. This section discusses these transformations in a nut shell and mentions the advantages offered by them.

3.1 Log-Gabor transform

Since long, Gabor filters have been a traditional choice for feature extraction as they offer good and simultaneous localization of spatial and frequency information. However, there are two main limitations associated with them. Firstly, the maximum bandwidth of a Gabor filter is limited to approximately one octave and secondly, they are not considered optimal for covering broad spectral information with maximal spatial localization. Log-Gabor function is an alternative to the Gabor function proposed by Field [16]. Log-Gabor filters have Gaussian transfer functions measured on logarithmic frequency scale. The filters are constructed in polar coordinate system in terms of radial and angular components. These components determine the frequency band and orientation at which filter is constructed. The frequency response of the radial and angular component is described in (1) and (2), respectively.

$$G_r(r) = exp\left(\frac{log(r/f_0)}{2\sigma_r^2}\right) \tag{1}$$

$$G_\theta(\theta) = exp\left(\frac{-(\theta-\theta_0)^2}{2\sigma_\theta^2}\right) \tag{2}$$

Due to singularity of log function at the origin, analytic expression for log-Gabor function cannot be constructed in spatial domain. They need to be constructed in the frequency domain and are numerically defined in spatial domain via inverse Fourier transform. The overall transfer function is constructed by multiplying the frequency response of these two components and expressed as

$$\begin{aligned} G(r,\theta) &= G_r(r).G_\theta(\theta) \\ &= exp\left(\frac{log(r/f_0)}{2\sigma_r^2}\right).exp\left(\frac{-(\theta-\theta_0)^2}{2\sigma_\theta^2}\right) \end{aligned} \tag{3}$$

where (r,θ) represents polar coordinates and f_0 is the center frequency of the filter. Let $minWave$ is wavelength of the smallest scale filter and $mult$ is the scaling factor between successive filters. The smallest value that can be assigned to $minWave$ is Nyquist wavelength of 2 pixels. Filtering at this wavelength suffers from considerable aliasing, so it is suggested to keep the minimum value to 3 pixels or above. The minimum frequency is determined by the wavelength of the largest scale filter. Let the number of filter scales be n, then the wavelength of the largest scale filter can be computed as $maxWave = minWave \times mult^n$. The minimum frequency is computed as $f_0 = 1/maxWave$.

The factors θ_0, σ_r, and σ_θ represent the orientation angle, the scalar bandwidth, and the angular bandwidth of the filter, respectively. The scalar bandwidth σ_r of the filter is set by specifying the ratio of the standard deviation of the radial filter. Small values of σ_r leads to larger bandwidth of filter. As determined empirically, parametric values of $\sigma_r = 0.75$, $mult = 1.6$ will result in filter bandwidth of approximately one octave, and $\sigma_r = 0.55$, $mult = 3$ will result in filter bandwidth of roughly two octaves [27]. For experimental purposes in this work, the spatial frequency domain is divided into 6 orientations ($m = 1, .., 6$) for each of the 4 scales ($n = 1, ..4$) resulting in a filter bank of $6 \times 4 = 24$ filters. To achieve fairly even spectral coverage of the log-Gabor filter bank at a bandwidth of two octaves, the values chosen for parameters are: $minWave = 3$, $mult = 3$, $\sigma_r = 0.55$. A value of $\sigma_\theta = 1.5$ results in approximately minimum overlap needed between successive filters to obtain an even spectral coverage.

Let I be the original image, whose features are to be extracted using log-Gabor filters. The image is transformed to the frequency domain using Fast Fourier Transform (FFT).

The Fourier transformed image is then multiplied with the log-Gabor frequency response at different scales (n) and orientations (m). The inverse Fourier transform of multiplied resultant (filtered image) at different values of (n, m) is computed to obtain the log-Gabor transformed image as

$$I^t_{m,n} = inverseFFT\left(I^f(\mu, \nu).F_{m,n}(\mu, \nu)\right), \tag{4}$$

where $I^f(\mu, \nu)$ is the Fourier transform of the input image I; $F_{m,n}(\mu, \nu)$ is the frequency response of log-Gabor filter and $I^t_{m,n}$ is the log-Gabor transformed image at orientation m and scale n. $I^t_{m,n}$ is a complex value matrix, with real (Re) and imaginary(Im) parts. Based on these two parts, the magnitude and phase patterns of log-Gabor transformed image can be computed as

$$F^{Mag}_{m,n} = \sqrt{Re\left(I^t_{m,n}\right)^2 + Im\left(I^t_{m,n}\right)^2} \tag{5}$$

$$F^{Phase}_{m,n} = \arctan^{-1}\left(\frac{Im\left(I^t_{m,n}\right)}{Re\left(I^t_{m,n}\right)}\right) \tag{6}$$

Various improvements and implementation based modifications are suggested in literature for efficient and fast signal processing using Gabor based filters which makes them useful for real life applications [1, 2, 59]. Various techniques that make use of Gabor and log-Gabor phase and magnitude patterns for feature extraction are described in [12, 52, 53]. For further enhancement of discriminablity, local patterns on phase and magnitude are computed using techniques like local phase quantization (LPQ) or local binary pattens (LBP) which are either directly used or spatial histograms are computed over them to form the final feature vector [37, 61, 62, 64, 66, 68]. As compared to Gabor filters, log-Gabor filters also handle variations due to scaling and rotations while using a comparatively smaller set of filter banks.

3.2 Random projection (RP)

Because of the information preservation property, RP has been widely used as a dimensionality reduction and privacy preserving tool. There are image and text data processing applications that use RP based dimensionality reduction such as face recognition [5, 19], clustering [25], data mining [40], and learning of mixture of Gaussian [14]. BioHashing is entirely based on RP for privacy protection of its feature vectors [24]. Other applications include [44, 57, 60].

Key concept of RP arises from the Johnson and Lindenstrauss lemma (*JL lemma*) [18]. *JL lemma* states that a set of a points in a high dimensional Euclidean space can be mapped down onto a k-dimensional subspace ($k \geq O(log(a/\epsilon^2))$), such that the distances between the points are approximately preserved (i.e., not distorted more than a factor of $(1 \pm \epsilon$, for $0 < \epsilon < 1$). The extent to which pair-wise distances between points before and after projection are preserved depends upon the column vector that constitutes the projection matrix R. As stated in *JL lemma*, these column vectors are required to be orthogonal to each other. Usually Gram Schmidt orthogonalization process is used to transform the columns of a random vector into orthogonal ones. Later it has been noted that the condition of orthogonality can be dropped while using random projections [22]. Thus, projection on normally distributed (or Gaussian distributed) random vectors having zero mean and unit variance is a distance preserving mapping with less computation costs. The following papers are suggested to be referred for usage, deeper insights, and mathematical proofs [5, 22, 55, 60].

4 The proposed approach

The proposed approach entwines multi-level transformations according to some user specific parameters to generate robust, secure, and revocable features. At signal level, the biometric image signal is distorted by projecting it on Gaussian random matrix. For efficient extraction of features, log-Gabor filtering is applied to the projected image whose phase and magnitude patterns are computed at multiple scales and orientations. The obtained phase and magnitude patterns are salted at feature level by XORing them with a random grid followed by non-linear median filtering, de-sampling, and binarization. The binary vectors for different scales and orientations are concatenated and classified using kernel discriminant analysis (KDA). The block diagram of the proposed approach is shown in Fig. 1.

Let X be a raw biometric image signal acquired at the sensor. It is preprocessed to remove noise and extract region of interest (ROI). Preprocessed sample is subjected to signal level distortions by user-specific Random Projections (RP) [5, 55, 60]. Let X^I is preprocessed image of dimension $d \times N$ and R is the user-specific projection matrix of dimension $k \times d$, where $k < d/2$. Column entries of R are independent random variables with the standard normal distribution having zero mean and unit variance. Projection of $X^I \in \Re^d$ on k-dimensional random subspace, X^{RP}, is computed as

$$X^{RP} = RX^I \tag{7}$$

Random projections have been proved to preserve the pair-wise distances between any two points after projecting them on low dimensional subspace. The dimension of X^{RP} is $k \times N$. As $k < d/2$, the template size reduces by at least 50 % or more. The projected image X^{RP} is subjected to log-Gabor transform using (4) and filtered images are obtained at $n = 4$ scales and $m = 6$ orientations. The magnitude and phase patterns for each filtered image are calculated using (5) and (6) and are denoted as $X^{mag}_{m,n}$ and $X^{ph}_{m,n}$ having $k \times N$ dimension. The next step fuses and salts phase and magnitude patterns with the help of a random grid RG to produce encrypted patterns for each scale and orientation combination by using (8).

$$XS_{m,n} = X^{mag}_{m,n} \oplus X^{ph}_{m,n} \oplus RG, \tag{8}$$

where $\oplus$ denotes XOR operation. RG is generated by randomly assigning a value between 0 to 255 with equal probability to each position $RG(x, y)$, $1 \le x \le k$, $1 \le y \le N$. XORing with random grids encrypts the visible phase and magnitude patterns and make them appear like random noise. As XOR is a linear operation, this step is essentially invertible. To make the salting of fused patterns non-invertible, 2-D median filtering is applied. Median

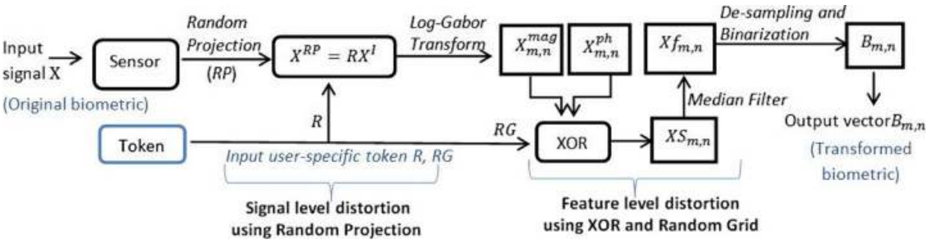


Fig. 1 Block diagram of the proposed approach

filters are non-linear spatial filters which reshuffle intensity values at each position in the salted pattern, $XS_{m,n}(x, y)$, by replacing it with the median value contained in its 5 × 5 neighborhood. The filtered image denoted as $Xf_{m,n}$ is normalized and reshaped as 1-D vector followed by binarization via thresholding. Adaptive thresholding determines a threshold value τ by calculating mean over a user's sample template and the vector is de-sampled by 50 %. De-sampled vector is quantized as 0 or 1 depending upon the threshold value τ. These binary features, $B_{m,n}$, are concatenated to form the final feature vector. De-sampling makes it computationally hard for an attacker to statistically determine the threshold value τ used for generating binary vectors.

KDA is performed to further reduce the dimensionality and extract the most discriminative information from feature vectors which are matched using Mahalanobis Cosine distances [4]. KDA computes a non-linear subspace from the training samples and uses it for learning. This helps in better classification of test samples [41]. In case of compromise, new templates can be generated from the same biometric sample by changing its user specific variables, i.e., random projection matrix R and/or random grid RG.

4.1 An illustrative example

For a sample image, the output images obtained at each step of the proposed approach as shown in Fig. 1 are illustrated in Fig. 2. Figure 2a shows 128 × 128 preprocessed face image. User specific Gaussian random matrix is of dimension 64 × 128. The projected image computed by (7) is 64 × 128 as shown in Fig. 2b. This projected image is subjected to log-Gabor transform, and magnitude and phase patterns are computed at 4 scales and 6 orientation as shown in Fig. 2c and d, respectively. Figure 2e shows the output of salted phase and magnitude patterns using random grid as defined in (8). It can be seen that the encrypted images appear like a random noise. Figure 2f shows the output after median filtering, which is de-sampled and binarized to enhance the security of biometric features.

4.2 Some relevant issues

Due to similarity preserving property of random projections [55], the projected biometric image sample at the sensor (signal level) is dimensionally reduced but does not loses

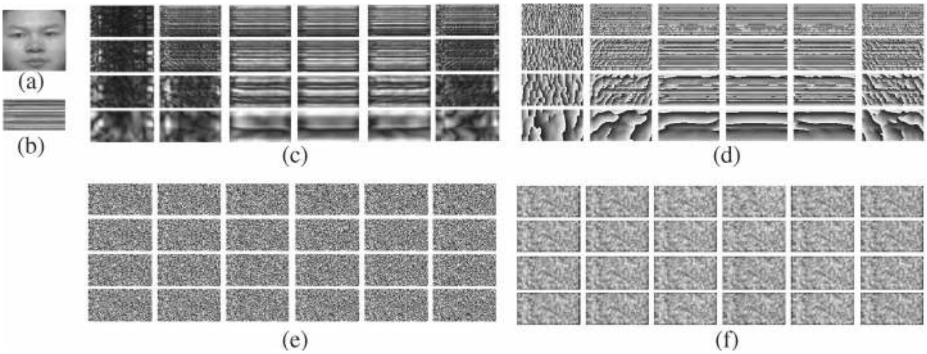


Fig. 2 Output images for multi-level transformations performed by the proposed approach **a** preprocessed image, **b** projected image X^{RP}, **c–d** log-Gabor magnitude $X^{mag}_{m,n}$ and phase $X^{ph}_{m,n}$ patterns at $n = 4$ scales and $m = 6$ orientations, **e** salted phase and magnitude patterns $XS_{m,n}$, and **f** output after median-filtering $Xf_{m,n}$

discriminative information. In the proposed approach, random projection applied before log-Gabor transform helps in significant dimension reduction of the output phase and magnitude patterns while preserving the discriminability of features. However, if random projection is used after log-Gabor, then it is required to be applied on every magnitude and phase pattern. It means that for $m = 4$ and $n = 6$, 48 RPs would be needed to introduce randomness and dimension reduction in patterns, while only one RP operation is required with the proposed approach. On the other hand, if we skip RP and only rely on single (feature) level transformation, the obtained phase and magnitude images as well as salted images will be of the same size as preprocessed image. Here, the advantages of multi-level transformations using RP over single level transformation are: (1) cheap and significant dimension reduction (discussed in Section 2.2); (2) increase in entropy of encrypted biometric template (further discussed in Section 5.4); and (3) increased security if the sensor and feature extractor are not located at the same physical location.

4.3 Non-invertibility offered by the proposed approach

Random projections enhance security and processing but they are essentially invertible. The novelty of the proposed approach lies in the XOR based salting method applied at the feature level. At the feature level, phase and magnitude patterns are salted using XOR operation with a random grid RG. XORing with random variables is a well known encryption technique. It does not distorts the biometric data but only encrypts it. Non-invertibility is achieved at the feature level by subjecting the salted patterns to non-linear median filtering. Non-linear median filtering shuffles these values in their neighborhood. The effectiveness of median filters in achieving non-invertibility is shown in Fig. 3. Instead of fused phase and magnitude patterns, a face image is used for better visualization in Fig. 3a. Figure 3b is a random grid RG of same dimension. When the face image in Fig. 3a is XORed with the RG in Fig. 3b, the result is shown in Fig. 3c. As XORing is invertible, if output image in Fig. 3c is XORed with RG in Fig. 3b, the original image is recovered. If we apply median filter on Fig. 3c, the output is Fig. 3d which contains the discriminative content of Fig. 3c. But if we try to invert it by XORing Fig. 3d with RG in Fig. 3b, the recovered results are shown in Fig. 3e. Although some feeble outlines and patterns are visible, it can be seen that the inverse obtained in Fig. 3e is distorted and looks noisy. De-sampling and binarization further strengthens the security and also reduces storage cost of the generated templates. Binary templates occupy very less storage as compared to other data types. The binarization of templates using adaptive threshold relies on statistical distribution of user features, thus preserving the overall information content of binary feature templates.

5 Experimental results and analysis

The performance of the proposed system is evaluated on visible as well as thermal biometrics. Thermal patterns are hidden under the skin and are unique to every individual. These are difficult to forge and are also unaffected by skin discolorations or age [43, 67].

5.1 Databases used for experimentation

Databases of various modalities used for experimentation are summarized in Table 1 and discussed below.

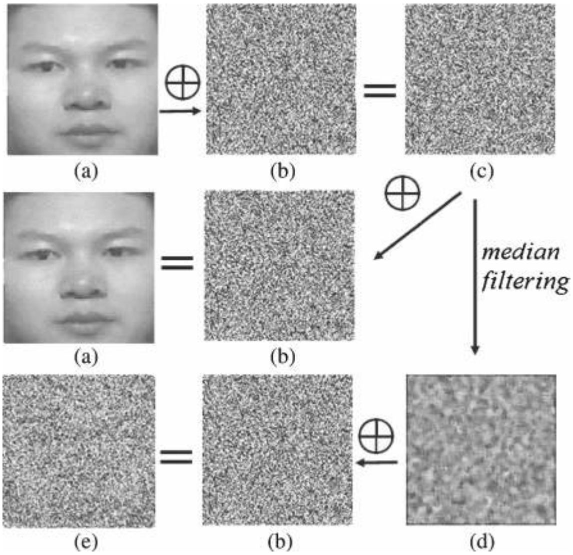


Fig. 3 Non-invertibility analysis (*first row*) Face image (**a**) XORed with random grid RG (**b**) results in (**c**); (*second row*) output (**c**) XORed with RG (**b**) recovers the original image (**a**); (*third row*) Median filtering of output (**c**) XORed with RG (**b**) recovers a lossy image (**e**)

5.1.1 Visible and thermal faces

In visible spectrum, the performance is evaluated on CASIA-Face V5 and ORL face databases. For near-wave infrared (NWIR) spectrum, CASIA NIR-VIS 2.0 and for long-wave infrared (LWIR) spectrum, IRIS face database is used. CASIA-Face V5 contains 2,500 color facial images from 500 subjects [8]. Originally, face image samples are 16 bit color BMP files of resolution 640 × 480. These images are converted to 8 bit gray scale images for experimentation. Olivetti Research Lab Database (ORL), contains 10 different

Table 1 Databases used for experimentation

Modality	Database	No. of subjects	Train samples per subject	Test samples per subject
Face	CASIA-Face V5 [8]	500	2	3
	ORL [45]	40	4	6
Thermal Face	CASIA NIR-VIS 2.0 [38]	500	2	3
	IRIS thermal/visible [23]	39	3	7
Palmprint	CASIA Palmprint [10]	301	3	5
	PolyU [46]	386	4	6
Palmvein	CASIA-MS V1 (940nm) [9]	200	2	4
Fingervein	SDUMLA-HMT [65]	212	2	4

Table 2 Matching performance for the proposed approach in stolen token and legitimate token scenario

Modality	Database	Stolen token (worst case)				Legitimate token (best case)			
		Multi-level		Single level		Multi-level		Single level	
		EER	DI	EER	DI	EER	DI	EER	DI
Face	CASIA V5	1.30 %	5.042	1.50 %	5.115	0.00 %	19.443	0.12 %	13.012
	ORL	0.59 %	6.439	0.77 %	6.310	0.00 %	17.823	0.14 %	14.284
Thermal Face	CASIA NIR V5	1.87 %	4.453	2.18 %	4.166	0.00 %	18.347	0.36 %	13.955
	IRIS thermal	1.38 %	6.424	1.55 %	6.423	0.00 %	21.383	0.01 %	15.542
Palmprint	CASIA Palmprint	1.98 %	5.226	2.15 %	5.112	0.00 %	19.872	0.09 %	12.543
	PolyU	0.59 %	5.869	0.95 %	5.736	0.00 %	20.443	0.06 %	11.987
Palmvein	CASIA-MS V1(940 nm)	4.66 %	3.812	4.95 %	3.122	0.00 %	19.345	0.56 %	10.544
Fingervein	SDUMLA-HMT	1.07 %	6.576	2.10 %	6.214	0.00 %	19.323	0.09 %	12.435

face images in grayscale for 40 subjects each of size 112 × 92 [45]. The images in both the databases are collected under varying light conditions, pose, facial expression, and facial details such as glasses/no glasses. The CASIA NIR-VIS consists of 3,940 visible and near infrared face images of size 640 × 480 from 197 subjects [38]. IRIS contains 4,228 pairs of thermal and visible faces of 39 subjects each of size 320 × 240 [23]. For each subject 10 thermal images are selected by restricting pose rotation angle between -45 degrees to +45 degrees. For visible and NWIR, ROI is extracted using triangle based face detection algorithm [39], while for LWIR IRIS thermal database it is performed with segmentation based elliptical region of interest [17].

5.1.2 Palmprint and palmvein

The performance is also evaluated on PolyU [46] and CASIA Palmprint [10] databases collected in visible spectrum. CASIA contains 5,239 hand images captured from 301 subjects. PolyU contains 7,752 grayscale images collected from 386 subjects with 10 palmprints captured at a particular session. CASIA multispectral palmprint (CASIA-MS V1) contains 7,200 grayscale palm images captured from each palm of 100 subjects for six different IR spectrum [9]. For each spectrum 6 images per subject are provided. Images acquired under 940-nm wavelength are used to form palmvein dataset. Rotation and translation issues are handled during ROI extraction by aligning all palmprints in the same direction and position [3]. Further, contrast limited adaptive histogram equalization (CLAHE) is applied to enhance palmvein images [20].

5.1.3 Fingervein

A publicly available SDUMLA-HMT fingervein database [65] is used to study the performance on fingervein biometric. It contains 320 × 240 fingervein images of 106 subjects. A total of 3,816 images are collected as 6 samples each for index finger, middle finger, and ring finger of both the hands. An edge detection algorithm is used to extract ROI [20] and cropping is performed using edge points and horizontal lines passing through them. Extracted ROI is enhanced with CLAHE.

Table 3 Matching performance for existing non-cancelable log-Gabor based approaches

Modality	Database	LGM		LGP		LBPLGM		LPQLPM	
		EER	DI	EER	DI	EER	DI	EER	DI
Face	CASIA V5	0.65 %	5.107	1.92 %	4.769	0.67 %	5.469	3.33 %	3.918
	ORL	1.51 %	5.806	1.50 %	5.479	0.18 %	6.538	0.96 %	6.247
Thermal Face	CASIA NIR V5	1.33 %	5.014	2.01 %	4.612	1.23 %	5.248	3.34 %	3.984
	IRIS thermal	2.82 %	4.408	4.13 %	3.696	0.55 %	6.135	1.49 %	6.405
Palmprint	CASIA Palmprint	0.76 %	5.577	2.00 %	4.989	0.05 %	5.85	1.78 %	4.282
	PolyU	0.47 %	9.780	0.01 %	8.917	1.03 %	4.924	2.36 %	3.381
Palmvein	CASIA-MS V1(940 nm)	2.6 %	4.361	4.01 %	4.102	1.33 %	5.263	6.07 %	3.022
Fingervein	SDUMLA-HMT	1.98 %	6.665	2.02 %	7.014	1.14 %	7.097	2.02 %	5.790

5.2 Performance evaluation

Matching performance is evaluated on Equal Error Rates (EER) and Decidability Index (DI). DI measures separability of genuine and impostor classes and is defined as the normalized distance between means of Genuine (μ_G) and Impostor distributions (μ_I). EER is used to evaluate the accuracy of the system and DI measures the confidence in classifying patterns for a given classifier. Lower EER values indicate higher recognition accuracy, while higher DI values indicate better decidability in classification of genuine and impostor populations.

Matching performance of the proposed approach is evaluated in stolen token scenario (worst case) as well as legitimate token scenario (best case). In stolen token scenario an attacker is always in possession of users' specific keys. The stolen token scenario is simulated by assigning same keys, e.g., R and RG to each subject in the database. Matching is performed on transformed templates of each subject in every database for two cases: (1) multi-level transformations in the proposed approach where same R and RG assigned to all users and (2) single (feature) level transformations when we skip RP and same RG is assigned to all users. Legitimate key scenario is simulated by assigning different transformation parameters to each user in the database under two cases: (1) multi-level transformations in the proposed approach where both R and RG are different for each user and (2) single level transformations when we skip RP and each user has a different RG. The results are summarized in Table 2. It is expected that the system performance must not regress when it operates on transformed templates under stolen token scenario for both the cases. For comparison purposes, matching experiments are also performed on original templates using four efficient feature extraction techniques based on log-Gabor filters cascaded with KDA for learning and classification. These techniques are − Log-Gabor Magnitude Patterns (LGM) [53], Log-Gabor Phase Patterns (LGP) [52], Local Binary Patterns of Log-Gabor Magnitudes (LBPLGM), and Local Phase Quantization of Log-Gabor Phase patterns (LPQLGP) [68]. Table 3 reports the experimental results on original databases using LGM, LGP, LBPLGM, LPQLGP for different modalities and databases. The experimental results reported in Tables 2 and 3 are average EER and DI values obtained after performing a 5-fold cross validation which creates 5 different sets of training and testing database by shuffling samples. Table 1 only specifies the fixed number of samples that are used each time for creating training and testing sets for each database.

It can be observed that the matching performance (EER) of proposed approach under stolen token scenario (Table 2) for both the cases is comparable to non-cancelable log-Gabor based techniques (Table 3). DI values obtained from genuine and impostor mean and variance in stolen token scenario are sufficiently high which indicate good separability between templates in transformed domain and show that genuine impostor population in transformed domain is well distributed. The experimental results validate that the proposed approach transforms biometric templates while effectively preserving their discriminability and meets the performance evaluation criteria of cancelability under stolen token scenario.

Nearly 0 % EER and very high DI values are observed for all databases and modalities in legitimate token scenario for both the cases. This is due to the increase in inter-user variations because of different user-specific keys R and RG. The results given in Table 2 show that multi-level transformation in the proposed approach give better results than single level transformation not only in legitimate token scenario but also in stolen token scenario. The ROC curves for the schemes given in Tables 2 and 3 are shown in Fig. 4. For the proposed approach ROC curves are shown for stolen token scenario as legitimate token scenario is undoubtedly beats all non-cancelable log-Gabor based approaches by achieving nearly zero EER values. ROC curves also show that the performance of the proposed approach even in stolen token scenario is comparable with other non-cancelable log-Gabor based approaches. It is worth emphasizing here that these observations are true for five biometric modalities. Also, better matching results are observed for multi-level transformation in both stolen token and legitimate token scenario. This further establishes the usefulness of the proposed approach.

5.3 Changeability analysis

Changeability analysis evaluates revocability and diversity properties of the generated templates. If the transformed template of a user is compromised, new ones can be generated by changing the user-specific keys. The proposed approach associates two variables, RP matrix R and random grid RG, to the user token. At the signal level, changeability is trivial as changing random projection matrix R will transform the data into a new projection space. This section analyzes the changeability when RP matrix R is same for all users while only RG is changed to generate new transformation templates. Because of information preservation property of RPs, this condition is sufficient to analyze changeability for both multi-level and single level cases as only RG is changed to generate new transformed databases.

A set of transformed templates is computed using RG_0 in stolen token scenario (all users having same key RG_0), and the generated database is called original transformed templates OTT. Similarly, a new transformed database is generated using a different token RG_1 and considered as new transformed templates NTT. Matching is performed separately on each transformed database OTT and NTT and calculated EER over both the databases are found to be similar for each modality as reported in Table 4. This suggests that performance is not affected by changing RG. Also, new transformed templates NTT are matched against original transformed templates OTT and very high EER (nearly 50 %) are obtained which indicates non match between different transformed templates.

There are two desirable properties of population distribution for high revocability. Firstly, the pseudo-impostor distribution must closely resemble the impostor distribution and secondly, the genuine distribution must be well separated from the pseudo-impostor distribution [11]. To model pseudo-impostor distribution, the newly generated transformed templates NTT were matched against the original transformed templates OTT. The genuine scores, imposter scores, and pseudo-imposter scores are plotted for each database

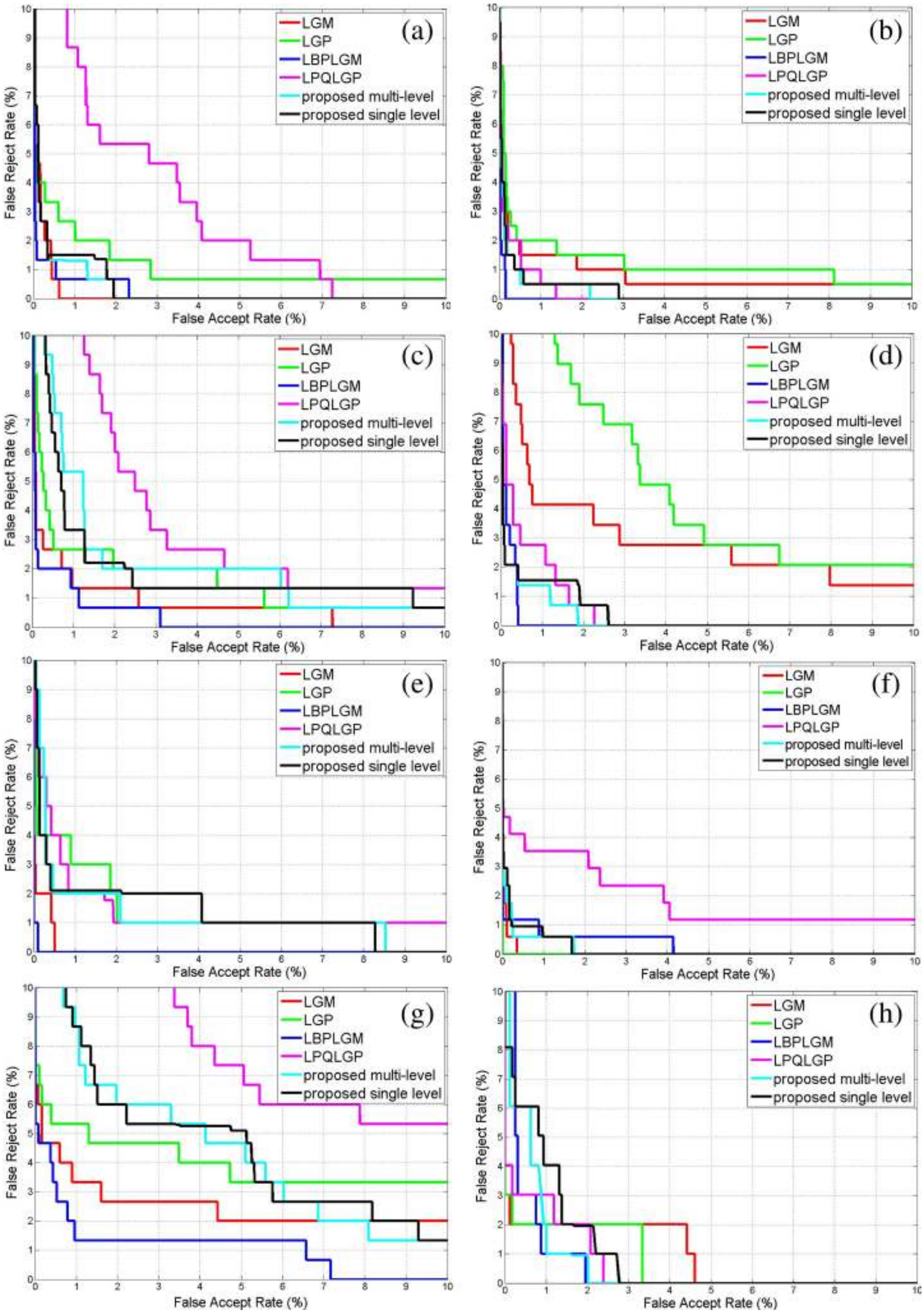


Fig. 4 ROC curves **a** CASIA V5 (face), **b** ORL (face), **c** CASIA NIR V5 (IR face), **d** IRIS (IR face), **e** CASIA (palmprint), **f** PolyU (palmprint), **g** CASIA-MS V1 (940nm) (palmvein), and **h** SDUMLA-HMT (fingervein)

Table 4 Genuine, imposter, and pseudo-imposter distribution and EER values

Modality	Database	Genuine		Imposter		Pseudo-imposter		EER	
		μ	σ	μ	σ	μ	σ	OTT	NTT
Face	CASIA V5	166.160	16.990	99.105	8.550	99.096	8.460	1.33 %	1.29 %
	ORL	188.670	10.730	98.080	17.150	98.120	16.120	0.51 %	0.54 %
Thermal Face	CASIA NIR V5	170.820	15.762	99.103	15.520	99.110	15.708	1.91 %	2.03 %
	IRIS	181.990	15.060	97.071	10.500	97.051	10.630	1.35 %	1.35 %
Palmprint	CASIA Palmprint	191.150	11.758	98.350	22.050	98.345	22.310	2.01 %	2.00 %
	PolyU	195.090	6.851	99.786	22.280	99.809	22.103	0.59 %	0.59 %
Palmvein	CASIA-MS V1(940 nm)	157.950	19.550	99.286	9.260	99.215	9.255	4.16 %	4.54 %
Fingervein	SDUMLA-HMT	186.310	18.640	92.651	14.080	92.658	14.080	1.16 %	1.10 %

as shown in Fig. 5. It can be seen that genuine score distribution is well separated from imposter score and pseudo-imposter score distribution. Also, the imposter and pseudo-imposter score distributions overlap each other with similar mean and standard deviation for every modality and database. Table 4 reports the obtained mean and standard deviation of the plotted scores. It implies that by using different user-specific keys, the resulting set of transformed templates differ hugely from each other.

In the similar way, we generated 100 new transformed database, $NTT_i = NTT_1, ..., NTT_{100}$, by assigning 100 different random grids $RG_i = RG_1, ..., RG_{100}$ to each database of each modality considered in this work. Thus, for each sample in a database, 101 cancelable templates (1 OTT +100 NTT) are generated. The same experimentation is performed between different pairs of transformed databases to model the pseudo-impostor populations and similar results are observed.

5.4 Vulnerability to correlation attacks

The revocable templates are created by changing the transformation parameter or the function itself. However, these transformed templates must not correlate to reveal any information about the original template. Assume that an attacker obtains multiple revoked templates of different users, but does not have any knowledge about the associated token data used for generating them. Here is the possibility of an attack, where the attacker is able to utilize this knowledge to estimate any of the user-specific key variables.

Also, if an attacker obtains multiple revoked templates of a user and has knowledge about the associated token data used for generating them. Say, Q number of transformed templates are generated from the original template by varying the parameter(s) K_q. Given these Q transformed templates and their keys K_q, a prediction attack can also be simulated by the attacker to estimate a new transformed template by varying the value of parameter(s). To prevent such kind of information leakage it is desirable that the mutual information content between a set of transformed templates should be as low as possible. To determine if an attacker can obtain any information about the original template, the mutual information content between any two transformed templates X and Y is calculated as:

$$I(X;Y) = \sum_{x}\sum_{y} P(x,y) log \frac{P(x,y)}{P(x), P(y)}, \tag{9}$$

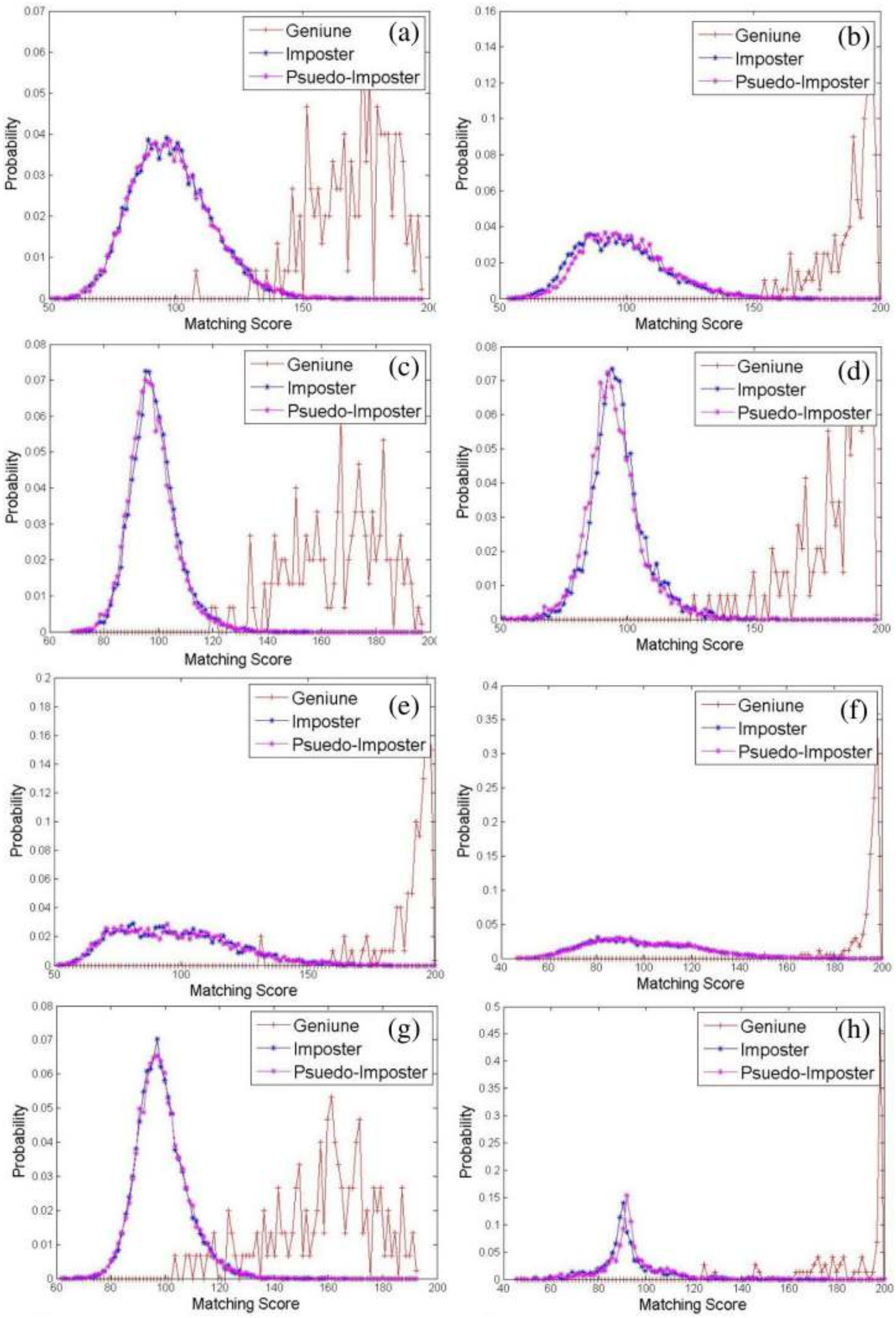


Fig. 5 Population distribution curves **a** CASIA V5 (face), **b** ORL (face), **c** CASIA NIR V5 (IR face), **d** IRIS (IR face), **e** CASIA (palmprint), **f** PolyU (palmprint), **g** CASIA-MS V1 (940nm) (palmvein), and **h** SDUMLA-HMT (fingervein)

where $P(x)$ and $P(y)$ are the marginal probabilities of x and y respectively, and $P(x, y)$ is the joint probability of x and y. Since the finally concatenated feature vectors have binary representation, the marginal probabilities of x and y can have values as $P(X = 0)$, $P(Y = 0)$, $P(X = 1)$, or $P(Y = 1)$. Therefore joint probability can be either of the four combinations of $P(X = 0, Y = 0)$, $P(X = 0, Y = 1)$, $P(X = 1, Y = 0)$ and $P(X = 1, Y = 1)$. The correlation among the different transformed templates should be minimal to prevent information leakage to the attacker. The proposed approach relies on multiple factors to generate transformed templates. These are projection matrix R and random grid RG. Also, new transformed templates can be generated by any of the three cases: Case (1): only R is changed, Case (2): only RG changed, and case (3): both R and RG are changed to generate new transformed templates.

To evaluate the correlation index, ten different transformed templates are generated for each database by changing user-specific parameters as specified for each of the three cases. Mutual information content I is calculated between each pair of transformed templates corresponding to the same biometric signal. The correlation index (CI) is the mean of all collected I values. Table 5 shows the CI values of binary templates for different modalities and databases. Here average value of $CI = 0.101$ means that two templates generated from the same biometric sample using different random keys share 10.1 % of mutual information and are slightly correlated. It is observed from Table 5 that case 3 offers higher resistance to correlation attacks by obtaining lowest CI values. This suggests that the multi-level transformation increases entropy of transformed template and minimizes the probability of information leakage.

5.5 Vulnerability to spoofing attacks

Multi-factor authentication by linking user-specific tokens to biometric authentication hardens the spoofing attack on the system. However, if we consider the stolen-token scenario where all user-specific transformation parameters are public, the proposed system is as much vulnerable to spoofing like any other non-cancelable biometric systems. To prevent spoofing, liveness detection algorithms can be incorporated at the sensor such as motion detection, eye blinking, random head and lip movements. Thermal biometrics like thermal face, palmvein, and fingerveins when used as input modality for biometric authentication aids automatic liveness detection. They are difficult to forge as they radiate patterns from blood vessels hidden under the skin and can reduce system's vulnerability to spoofing attacks.

Table 5 Correlation index values for different cases

Modality	Database	Correlation index (CI)		
		Case1	Case 2	Case3
Face	CASIA V5	0.101	0.113	0.008
	ORL	0.081	0.092	0.014
Thermal Face	CASIA NIR V5	0.120	0.125	0.007
	IRIS thermal	0.110	0.098	0.020
Palmprint	CASIA Palmprint	0.120	0.076	0.023
	PolyU	0.121	0.665	0.012
Palmvein	CASIA-MS V1	0.190	0.122	0.016
Fingervein	SDUMLA-HMT	0.135	0.782	0.019

6 Conclusion

A novel multi-level transformation based template protection scheme using random projection and log-Gabor filters is developed and discussed in this work. The proposed approach robustly extracts and transforms features to fulfill various criteria of the template protection method. The applicability of the approach is tested on various biometric modalities and results are reported after tuning the system for 5-fold cross validation of training and testing databases. Revocability and diversity properties of cancelable biometric features are experimentally verified. The analysis of genuine, impostor, and pseudo-impostor population distributions reveal that the proposed approach exhibits high changeability. It is also observed that the proposed approach is resistant to correlation attack, and unlike most biometric salting approaches, delivers good matching performance under stolen-token scenario.

References

1. Amayeh G, Tavakkoli A, Bebis G (2009) Accurate and efficient computation of gabor features in real-time applications. In: Advances in Visual Computing, Springer, pp 243–252
2. Areekul V, Watchareeruetai U, Tantaratana S (2004) Fast separable gabor filter for fingerprint enhancement. In: Biometric Authentication. Springer, pp 403–409
3. Aykut M, Ekinci M (2015) Developing a contactless palmprint authentication system by introducing a novel roi extraction method. Image Vis Comput 40:65–74
4. Beveridge R, Bolme D, Teixeira M, Draper B (2003) The csu face identification evaluation system users guide: version 5.0. Computer Science Department, Colorado State University 2 (3)
5. Bingham E, Mannila H (2001) Random projection in dimensionality reduction: applications to image and text data. In: Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining, pp 245–250
6. Bolle RM, Connell JH, Ratha NK (2002) Biometric perils and patches. Pattern Recogn 35(12):2727–2738
7. Boult TE, Scheirer WJ, Woodworth R (2007) Revocable Fingerprint biotokens: Accuracy and security analysis. In: Computer vision and pattern recognition, 2007. CVPR'07. IEEE Conference on, pp 1–8
8. CASIA-FaceV5 Biometrics Ideal Test. http://biometrics.idealtest.org
9. CASIA-MS-Palmprint V1 Biometrics Ideal Test. http://biometrics.idealtest.org
10. CASIA palmprint database Biometrics Ideal Test. http://biometrics.idealtest.org/downloadDB/
11. Chin YJ, Ong TS, Teoh ABJ, Goh K (2014) Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Inf Fusion 18:161–174
12. Chu R, Lei Z, Han Y, He R, Li SZ (2007) Learning gabor magnitude features for palmprint recognition. In: Computer Vision–ACCV 2007. Springer, pp 22–31
13. Connie T, Teoh A, Goh M, Ngo D (2005) Palmhashing: a novel approach for cancelable biometrics. Inf Process Lett 93(1):1–5
14. Dasgupta S (2000) Experiments with random projection. In: Proceedings of the Sixteenth conference on Uncertainty in artificial intelligence, Morgan Kaufmann Publishers Inc., pp 143–151
15. Farooq F, Bolle RM, Jea TY, Ratha N (2007) Anonymous and revocable fingerprint recognition. In: Computer vision and pattern recognition, 2007. CVPR'07. IEEE Conference on, pp 1–7
16. Field DJ (1987) Relations between the statistics of natural images and the response properties of cortical cells. JOSA A 4(12):2379–2394
17. Filipe S, Alexandre LA (2014) Algorithms for invariant long-wave infrared face segmentation: evaluation and comparison. Pattern Anal Applic 17(4):823–837
18. Frankl P, Maehara H (1988) The johnson-lindenstrauss lemma and the sphericity of some graphs. J Comb Theory B 44(3):355–362
19. Goel N, Bebis G, Nefian A (2005) Face recognition experiments with random projection. In: Defense and Security, International Society for Optics and Photonics, pp 426–437
20. Gonzalez RC, Woods RE, Eddins SL (2004) Digital image processing using MATLAB. Pearson Education India
21. Hirata S, Takahashi K (2009) Cancelable biometrics with perfect secrecy for correlation-based matching. In: Advances in Biometrics. Springer, pp 868–878

22. Indyk P, Motwani R (1998) Approximate nearest neighbors: towards removing the curse of dimensionality. In: Proceedings of the thirtieth annual ACM symposium on Theory of computing, pp 604–613
23. IRIS thermal/visible face database University of Tennessee. http://www.cse.ohio-state.edu/otcbvs-bench/
24. Jin ATB, Ling DNC, Goh A (2004) Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recogn 37(11):2245–2255
25. Kaski S (1998) Dimensionality reduction by random mapping: Fast similarity computation for clustering. In: Neural networks proceedings, 1998. IEEE world congress on computational intelligence. The 1998 IEEE international joint conference on, IEEE, vol 1, pp 413–418
26. Kaur H, Khanna P (2015) Biometric template protection using cancelable biometrics and visual cryptography techniques. Multimedia Tools and Applications 1–29
27. Kovesi P (1999) Image features from phase congruency. Videre: J Comput Vis Res 1(3):1–26
28. Lacharme P, Cherrier E, Rosenberger C et al (2013) Preimage attack on biohashing. In: International Conference on Security and Cryptography (SECRYPT)
29. Lee C, Kim J (2010) Cancelable fingerprint templates using minutiae-based bit-strings. J Netw Comput Appl 33(3):236–246
30. Lee Y, Chung Y, Moon K (2009) Inverse operation and preimage attack on biohashing. In: Computational intelligence in biometrics: theory, Algorithms, and Applications, 2009. CIB 2009. IEEE Workshop on, pp 92–97
31. Leng L, Teoh ABJ (2015) Alignment-free row-co-occurrence cancelable palmprint fuzzy vault. Pattern Recogn 48(7):2290–2303
32. Leng L, Zhang J (2011) Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security. J Netw Comput Appl 34(6):1979–1989
33. Leng L, Zhang J (2013) Palmhash code vs. palmphasor code. Neurocomputing 108:1–12
34. Leng L, Zhang J, Khan M, Bi X, Ji M (2010) Cancelable palmcode generated from randomized gabor filters for palmprint protection. Sci Res Essays 6(4):784–792
35. Leng L, Li M, Teoh ABJ (2013) Conjugate 2dpalmhash code for secure palm-print-vein verification. In: Image and signal processing (CISP), 2013 6th international congress on, IEEE, vol 3, pp 1705–1710
36. Leng L, Teoh ABJ, Li M, Khan MK (2014) Analysis of correlation of 2dpalmhash code and orientation range suitable for transposition. Neurocomputing 131:377–387
37. Li J, Sang N, Gao C (2014) Log-gabor weber descriptor for face recognition. In: Computer vision-ACCV 2014 Workshops. Springer, pp 541-553
38. Li SZ, Yi D, Lei Z, Liao S (2013) The casia nir-vis 2.0 face database. In: Computer vision and pattern recognition workshops (CVPRW), 2013 IEEE Conference on, pp 348–353
39. Lin C, Fan KC (2001) Triangle-based approach to the detection of human face. Pattern Recogn 34(6):1271–1284
40. Liu K, Kargupta H, Ryan J (2006) Random projection-based multiplicative data perturbation for privacy preserving distributed data mining. IEEE Trans Knowl Data Eng 18(1):92–106
41. Lu J, Plataniotis KN, Venetsanopoulos AN (2003) Face recognition using kernel direct discriminant analysis algorithms. IEEE Trans Neural Netw 14(1):117–126
42. Maiorana E, Campisi P, Neri A (2011) Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system. In: Systems conference (SysCon), 2011 IEEE International, pp 495–500
43. Mulyono D, Jinn HS (2008) A study of finger vein biometric for personal identification, Biometrics and Security. In: Technologies, 2008. ISBAST 2008. International Symposium on, pp 1–8
44. Ngo DC, Teoh AB, Goh A (2006) Biometric hash: high-confidence face recognition. IEEE Trans Circuits Syst Video Technol 16(6):771–775
45. ORL face database AT&T Laboratories Cambridge. http://www.cl.cam.ac.uk/
46. PolyU palmprint database The Hong Kong Polytechnic University. http://www4.comp.polyu.edu.hk/~biometrics/
47. Quan F, Fei S, Anni C, Feifei Z (2008) Cracking cancelable fingerprint template of ratha. In: Computer science and computational technology, 2008. ISCSCT'08. International symposium on, vol 2, pp 572–575
48. Ratha N, Connell J, Bolle RM, Chikkerur S (2006) Cancelable biometrics: a case study in fingerprints. In: Pattern recognition, 2006. ICPR 2006. 18th international conference on, vol 4, pp 370–373
49. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634
50. Savvides M, Kumar BV, Khosla PK (2004) Cancelable biometric filters for face recognition. In: Pattern recognition, 2004. ICPR 2004. Proceedings of the 17th international conference on, vol 3, pp 922–925

51. Soutar C, Roberge D, Stoianov A, Gilroy R, Kumar BV (1998) Biometric encryption using image processing. In: Photonics West'98 Electronic Imaging, International Society for Optics and Photonics, pp 178–188
52. Štruc V, Pavešić N (2010) The complete gabor-fisher classifier for robust face recognition. EURASIP Journal on Advances in Signal Processing 2010:31
53. Štruc V, Pavešić N (2009) Gabor-based kernel partial-least-squares discrimination features for face recognition. Informatica (Vilnius) 20(1):115–138
54. Sutcu Y, Sencar HT, Memon N (2005) A secure biometric authentication scheme based on robust hashing. In: Proceedings of the 7th workshop on Multimedia and security, pp 111–116
55. Teoh A, Jin B, Connie T, Ngo D, Ling C (2006) Remarks on biohash and its mathematical foundation. Inf Process Lett 100(4):145–150
56. Teoh ABJ, Ngo DCL (2006) Biophasor: Token supplemented cancellable biometrics. In: Control, Automation, Robotics and Vision, 2006. ICARCV'06. 9th International Conference on, pp 1–5
57. Teoh ABJ, Yuang CT (2007) Cancelable biometrics realization with multispace random projections. IEEE Trans Syst Man Cybern B Cybern 37(5):1096–1106
58. Uludag U, Pankanti S, Prabhakar S, Jain AK (2004) Biometric cryptosystems: issues and challenges. Proc IEEE 92(6):948–960
59. Wang X, Shi BE (2010) Gpu implemention of fast gabor filters. In: Circuits and systems (ISCAS), proceedings of 2010 IEEE International Symposium on, pp 373–376
60. Wang Y, Plataniotis KN (2010) An analysis of random projection for changeable and privacy-preserving biometric verification. IEEE Trans Syst Man Cybern B Cybern 40(5):1280–1293
61. Xie S, Shan S, Chen X, Chen J (2010) Fusing local patterns of gabor magnitude and phase for face recognition. IEEE Trans Image Process 19(5):1349–1361
62. Yang B, Chen S (2013) A comparative study on local binary pattern (lbp) based face recognition: Lbp histogram versus lbp image. Neurocomputing 120:365–379
63. Yang W, Hu J, Wang S, Yang J (2013) Cancelable fingerprint templates with delaunay triangle-based local structures. In: Cyberspace Safety and Security. Springer, pp 81–91
64. Yi J, Su F (2014) Histogram of log-gabor magnitude patterns for face recognition. In: Acoustics, speech and signal processing (ICASSP), 2014 IEEE International Conference on, pp 519–523
65. Yin Y, Liu L, Sun X (2011) Sdumla-hmt: a multimodal biometric database. In: Biometric Recognition. Springer, pp 260–268
66. Zhang B, Shan S, Chen X, Gao W (2007) Histogram of gabor phase patterns (hgpp): A novel object representation approach for face recognition. IEEE Trans Image Process 16(1):57–68
67. Zhou Y, Kumar A (2011) Human identification using palm-vein images. IEEE Trans Inf Forensics Secur 6(4):1259–1274
68. Zhou SR, Yin JP, Zhang JM (2013) Local binary pattern (lbp) and local phase quantization (lbq) based on gabor filter for face representation. Neurocomputing 116:260–264

Harkeerat Kaur received BE degree from JEC, Jabalpur (2012). Currently, she is pursuing PhD in computer science at Indian Institute of Information Technology, Design and Manufacturing, Jabalpur, India. Her research interests include computer vision, image processing, biometrics, and visual cryptography.

Pritee Khanna received PhD degree in Computer Science from Kurukshetra University Kurukshetra, India (2004). Currently she is working as an Associate Professor of Computer Science & Engineering in Indian Institute of Information Technology, Design and Manufacturing, Jabalpur, India. She has published over 50 research papers in journals and conferences of repute. Her research interests include human-computer interaction, content based image retrieval, and biometrics.