Random Distance Method for Generating Unimodal and Multimodal Cancelable Biometric Features

Harkeerat Kaur and Pritee Khanna

***Abstract*— The cancelable biometric-based template protection method proposed in this paper addresses security and privacy concerns emerging from the phenomenal usage of biometric systems. Cancelable biometric transforms the original biometric identity of a user to a pseudo-biometric identity that is used for storage and matching purposes. The use of pseudo-identity mitigates privacy risks and allows revocability in case of compromise. This paper proposes a novel template transformation technique named random distance method which not only generates discriminative and privacy preserving revocable pseudo-biometric identities, but also reduces their size by 50%. Extensive experimentation is performed to analyze recognition and protection performance on unimodal and multimodal pseudo-identities generated with various biometric modalities such as face, thermal face, palmprint, palmvein, and fingervein. It is observed that the matching performance obtained with the proposed cancelable templates in the worst-case is closer to the performance achieved in the original domain. Also, multimodal cancelable biometric templates generated with the proposed method are observed for improved performance. Furthermore, the proposed approach is successfully analyzed for non-invertibilty, unlinkability, as well as its resistance for various types of attacks like attacks via record multiplicity, dictionary, false accepts, and brute force.**

***Index Terms*— Cancelable biometrics, revocable, random distance method, multimodal.**

I. Introduction

BIOMETRIC authentication systems are in use for providing secure access to conventional as well as security critical applications. Most of the biometric information is stored as digital entities which are at the risk due to hacking and other malicious activities. Physical/digital biometric artifacts can be easily constructed from stolen identities to obtain illegitimate access. Also, loss of a biometric identity at some common and less secure application may incapacitate its usage in a high security application. With increase in network and cloud based applications, cyber crimes against identity frauds have also increased. Thus, "*security of biometric information*" has become as important and essential as ensuring "*security using biometric information*". Apart from security, there are certain privacy issues stemming from the use of biometrics. Covert surveillance, sharing of biometric databases without users' consent and cross-matching them are some forms of privacy intrusion attacks. Loss of biometric identity threatens our security, invokes social and financial losses, invades people's privacy, and thereby produces negative emotional impact on victims. Security and protection of biometric identities is of significant importance in the today's digital world as the number of biometrics are limited.

Cancelable biometrics generates pseudo-biometric identities as protected version of original biometric identities using some transformation function and user-specific secret key/auxiliary data [1]. It provides high level privacy, security, and revocability to biometrics by performing storage and matching in the transformed domain. This work proposes a novel template transformation technique named as '*Random Distance Method*' that not only generates non-invertible, revocable, and diverse pseudo-identities, but also reduces it size by 50%. The method maps biometric features as points on the Cartesian space and calculates its distance from some random points defined according to some user-specific secret key/token. The proposed approach is tested for unimodal amd multimodal transformed templates generated for various modalities like face, palmprint, palmvein, and fingervein.

The work is organized as follows. Section II provides an insight to the existing transformation techniques and outlines motivation for the proposed work. Section III discusses random distance concept and the proposed template protection approach. Section IV provides illustrative examples and addresses some relevant issues. Experimental analysis is given in Section V. Finally, the work is concluded in Section VI.

II. Cancelable Biometrics

The basic enrollment and authentication process under the cancelable biometric setup is discussed here. At enrollment, the original biometric identity (B) of a user is transformed with the help of some secret user-specific key in a non-invertible and discriminability preserving fashion to generate a transformed feature/pseudo-biometric identity (PI). The PI is stored in the database and the key is provide to the user in a tokenized format such as a smart card. At authentication, user inputs his probe biometric (B') and token, which are transformed in a similar manner to generate the query template (PI'). The stored 'reference' and 'query' templates are matched in the transformed domain to declare a match or non-match. In case of an attack only pseudo-identity is compromised which can be regenerated any time by changing the

Manuscript received November 2, 2017; revised March 15, 2018 and May 25, 2018; accepted June 18, 2018. Date of publication July 12, 2018; date of current version September 13, 2018. This work was supported by BRNS, Department of Atomic Energy, Government of India, under Grant 36(3)/14/58/2016-BRNS. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Tanya Ignatenko. *(Corresponding author: Pritee Khanna.)*

The authors are with the Department of Computer Science and Engineering, PDPM Indian Institute of Information Technology, Design and Manufacturing at Jabalpur, Jabalpur 482005, India (e-mail: pkhanna@iiitdmj.ac.in).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2018.2855669

transformation function or key. Further, numerous pseudo-identities can be generated from a single sample for usage across different applications by changing the transformation function and/or key, thereby preventing cross-matching and other attacks. This fulfills the important template protection properties namely *non-invertibility*, *revocability*, and *diversity* [1]. Transformation techniques can be classified as *biometric salting* and *non-invertible transforms*. Biometric salting distorts templates by blending them with auxiliary data, which is often followed by some additional operations to achieve non-invertibility. Non-invertible transforms are surjective one way functions, where user-key and biometric are input as parameters to a function which acts like an agent. Biometric salting techniques are further classified as *Random Projection* (RP), *Random Convolution*, and *Random Noise* based techniques.

Random Projection (RP) Based Transformations are most widely used salting techniques due to its discriminability preserving properties. It salts biometric data by projecting it on a random-subspace such that the pair-wise distances between points before and after projection are approximately preserved. Jin *et al.* (2004) [2] proposed BioHashing, where the projection sub-space is defined by orthonormal random matrices. The projected templates are quantized in order to generate non-invertible binary codes. However, pre-image attacks are possible if the binary codes and projection matrix are simultaneously known to the attacker [3]. Teoh and Yaung (2007) [4] proposed Multi-space Random Projection (MRP), a variant of BioHashing, to address the stolen token scenario. Wang and Plataniotis (2010) [5] appended a vector translation concept to improve changeability and non-invertibility of transformed templates. MRP with score fusion [6], multiple high dimension random projection [7], and sectored random projections [8] are some other random projection variants.

Random Convolution Based Transformations convolve biometric signal with random kernel to generate transformed templates. Savvides *et al.* (2004) [9] transformed face images by convolving those with random kernels. BioConvolving proposed by Maiorana *et al.* (2010) [10] uses random user-specific key to divide the original feature into fixed sized segments that are convolved later. However, discriminability preservation is not justified for both the approaches in stolen token scenario. Further, if convolution kernel and key are known, then deconvolution attempts may tend to compromise invertibility of the approach. Wang and Hu (2014) [11] used curtailed circular convolutions to generate non-invertible cancelable fingerprints with good matching performance, but the scheme is vulnerable to attacks via record multiplicity (ARM).

Random Noise Based Transformations distort templates by appending random patterns or noise signals. Teoh and Ngo (2006) [12] proposed BioPhasoring, which salts biometric template by converting it to a complex number. The original feature forms the real part and a random noise signal is assigned to the imaginary part. Phase of the complex vector forms non-invertible transformed template. Zuo *et al.* (2008) [13] generated cancelable iris patterns using two new salting techniques, namely, GRAY and BIN salting which are subjective to inverse attacks if the salting parameter is known. GRAY salting (template based salty noise) adds random noise patterns to a biometric template at image level, while BIN salting (code based salty noise) extracts binary features from the input image which are salted using binary patterns.

Non-Invertible Transformations Modify biometric data by mapping it to a new random subspace such that inverse mapping is not possible. Ratha *et al.* (2007) [1] proposed Cartesian, polar, and surface folding transforms for mapping minutiae features into random points in a revocable manner. Later, Quan *et al.* (2008) [14] proved that these transforms are invertible when transformed templates and transformation parameters are known simultaneously. Farooq *et al.* (2007) [15] and Lee and Kim (2010) [16] obtained cancelable bit strings from minutiae features where each cell of the array was assigned 0/1 depending upon the minutiae point lying in that cell or not. As the technique involves many-to-one mapping to achieve non-invertibility, it tends to compromise discriminability. Also, non-invertibility can be compromised when the bit string and user-specific key are known to the attacker. Yang *et al.* (2013) [17] extracted local structures of minutiae features using Delaunay triangulation which were subjected to non-invertible polar transformation to generate cancelable templates. The resulting distortions reduce performance and the scheme is susceptible to ARM. Wang *et al.* (2017) [18] proposed a partial discrete Fourier transform-based cancelable fingerprint templates using zoned minutiae pairs to get good performance as the local structures of minutiae points preserve discriminability after non-invertible distortions. Implementation of these techniques is limited to fingerprint modality.

Dwivedi *et al.* (2016) [19] generated cancelable iris templates, where some consistent bits from extracted features are used to generate a decimal encoded vector which is mapped using a look-up table. But the mapping can be inverted if look-up table and transformation parameters are known. Lai *et al.* (2017) [20] proposed Indexing-First-One (IFO) hashing that maps real-valued iris features into discrete index hashed codes. Another scheme proposed by Jin *et al.* (2017) maps real-valued fingerprint features into discrete index (max ranked) hashed codes. It is based on locality sensitive hashing (LSH) known as Index-of-Max (IoM) hashing [21]. Both IFO and IoM hashing provide good matching performance and analysis under non-invertibilty, ARM, and false accept attack.

Multibiometric Cancelable Schemes extend cancelability to multimodal systems for increased security and accuracy requirements. Multimodal systems fuse information at *score level*, *decision level* or *feature level*. Nanni and Lumini (2006) [22] utilized BioHashing to generate transformed face and fingerprint templates and analyzed their score level fusion for performance. Maiorana *et al.* (2011) [10] proposed score level fusion of transformed signature templates generated using BioConvolving for improving system performance. De Paula Canuto *et al.* (2012) [23] performed decision level fusion on cancelable fingerprint and signature templates. Fingerprint templates are transformed using BioHashing, whereas signature templates are transformed using BioConvolving.

Paul and Gavrilova (2012) [24] proposed a random cross folding method to generate multimodal cancelable templates

by performing feature level fusion on face and ear modalities. The original features belonging to each modality were divided into two equal parts according to some pseudo-random key. These parts were crossed over to form two folds that are transformed using orthonormal random projections and the results were combined to form cancelable templates. The authors also proposed multi-fold random projection for improving recognition performance [25]. Paul *et al.* (2014) [26] proposed multi-order cancelable transform consisting of random cross over method, random projection, and feature selection for generating multimodal (face and ear) cancelable templates. Along with enhanced performance, the system works with situation awareness when an attacker tries to make an illegitimate access. Rathgeb and Busch (2014) [27] transformed iris templates belonging to both eyes of a single subject using adaptive bloom filters, which are fused at feature level. Although the method provides improved performance, but the transformed templates can be linked. Chin *et al.* (2014) [28] proposed feature level fusion of fingerprint and palmprint templates by arranging them in a form of random rectangles defined by user-specific key and extracted statistical features. Gomez-Barrero *et al.* (2018) [29] proposed weighted feature level fusion of protected templates belonging to face and fingervein as well as face and iris. Protected templates are generated by using bloom filters and fused with OR operation.

Thus, designing a cancelable template transformation technique fulfilling the desired criteria of diversity, revocability, and non-invertibility without compromising performance is a challenging task. Also, template size depends on the size of acquired biometric image and the feature extraction process. Some efficient features extraction techniques like Gabor and wavelet filters operate on the image at multiple resolutions which may significantly increase template size. Only random projection (RP) based techniques [4]–[6] are found to be the most popular and extensively used for dimension reduction of transformed features due to their distance preserving property. But to achieve it, RP based methods generate random matrices having some special distribution. Also, projection operation requires complex multiplications which increases computation cost. Along with accuracy performance, the system must be analyzed for privacy issues concerning the leakage of information about original data and security against illegitimate access. For most of the approaches a thorough analysis of linkability attacks, pre-image attacks using leaked transformed template and key, and statistical attacks is not available.

The proposed concept of *Random Distance Method* is used to develop a feature transformation that generates *privacy preserving*, *performance preserving*, *revocable*, *non-invertible*, and *dimensionally reduced* cancelable biometric features. Along with better performance in the worst and best-case scenarios for various biometric modalities, the proposed system is shown resistant to leakage of original information when transformed template and/or transformation function/key are known to the attacker. Unlinkability is established according to latest benchmark [30]. Vulnerability of the proposed scheme against attacks via record multiplicity and security against illegitimate access using dictionary attack and False accept masquerading attack is also justified. Hence the scheme can be used to ensure security and privacy for industrial and commercial applications. Being token supplemented, the scheme is highly suitable for granting access to high security systems like banking, ATM, military applications, and network and cloud based applications involving remote authentications.

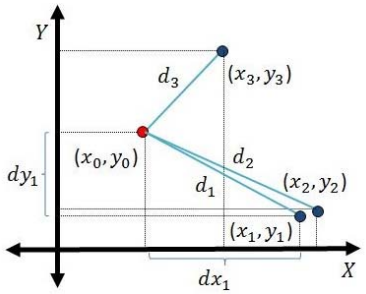

Fig. 1. The concept of random distance method.

III. Biometric Salting Using Random Distances

A. Random Distance Method (RDM)

Let a feature vector fv be represented as a point in the Cartesian coordinate system. It is proposed to use the distance of fv from some random point for matching purposes. The concept is illustrated in Fig. 1. Let the feature vector be divide into two equal halves such that the j^{th} feature belonging to the first half maps as the abscissa, and the corresponding feature at j^{th} position in the second half maps as the ordinate to define a point in the Cartesian space as $(x, y) \in fv$. Let (x_1,y_1), (x_2,y_2), and (x_3,y_3) are such point representations belonging to three different feature vectors fv_1, fv_2, and fv_3; and (x_0, y_0) is a random point derived from user-specific key. Assuming that the same key is assigned to each user (worst-case scenario), Euclidean distances d_1, d_2, and d_3 between feature points and random point are used as transformed features. If the feature vectors fv_1 and fv_2 belong to the same user, then the difference in their values would be small, i.e., $||x_1 - x_2|| < \delta$ and $||y_1 - y_2|| < \delta$, then it can be shown that $d_2 - d_1 \propto \delta$.

To Prove: $d_2 - d_1 \propto \delta$

Proof: Let $||x_2 - x_1|| = \delta$ and $||y_2 - y_1|| = \delta$

$dx_1 = x_0 - x_1, dy_1 = y_0 - y_1, dx_2 = x_0 - x_2, dy_2 = y_0 - y_2$

Therefore, $dx_2 - dx_1 = (x_0 - x_2) - (x_0 - x_1) = x_1 - x_2 = \delta$

Similarly, $dy_2 - dy_1 = (y_0 - y_2) - (y_0 - y_1) = y_1 - y_2 = \delta$

Also, $d_1 = dx_1^2 + dy_1^2$ and $d_2^2 = dx_2^2 + dy_2^2$

$d_2^2 = (dx_1 + \delta)^2 + (dy_1 + \delta)^2 = d_1^2 + 2\delta(\delta + dx_1 + dy_1)$

$d_2 - d_1 = 2\delta\frac{(\delta + dx_2 - \delta + dy_1)}{d_2 + d_1} = 2\delta\frac{(dx_2 + dy_1)}{d_2 + d_1}$

From the triangle properties, $dx_2 < d_2$ and $dy_1 < d_1$

Hence $dx_2 + dy_1 < d_2 + d_1$ and $\delta\frac{(dx_2 + dy_1)}{d_2 + d_1} < \delta$

Thus $d_2 - d_1 < \kappa\delta$ for some constant κ,

Hence Proved

If fv_1, fv_3 belong to different users, then the difference between their values would be large, i.e., $||x_3 - x_1|| < \Delta$ and $||y_3 - y_1|| < \Delta$, such that $\Delta > \delta$. Similarly it can be shown that $(d_3 - d_1) \propto \Delta$ for the same constant κ. Thus, inter and intra-user variations are maintained using RDM.

B. Feature Extraction Using Log-Gabor Filters:

Log-Gabor filters are used here to extract features of a preprocessed biometric image at various frequency resolutions [31]. Log-Gabor filters are Gaussian transfer functions over logarithmic frequency scale composed of radial (r) and angular components (θ) defined in polar coordinate system as $G(r,\theta) = exp\left(\frac{log(r/f_0)}{2\sigma_r^2}\right).exp\left(\frac{-(\theta-\theta_0)^2}{2\sigma_\theta^2}\right)$, where f_0 is the center frequency of the filter. Let the number of filter scales be n, then center frequency f_0 can be computed as $f_0 = 1/minWave \times mult^n$. Here, frequency domain is resolved at 4 scales ($n = 1...4$) and 6 orientations ($m = 1...6$) for each scale, resulting in a filter bank of 24 filters and parameters are set as $\sigma_r = 0.55$, $\sigma_\theta = 1.5$, $mult = 3$, and $minWave = 3$. Let I be $M \times N$ biometric image preprocessed for noise removal and ROI extraction. The responses at multiple resolutions are calculated by multiplying the Fast Fourier Transform (FFT) of image with filter response at n scales and m orientations. The filtered image is then obtained by computing the inverse FFT of multiplied resultant. For each scale and orientation, the obtained magnitude patterns are reshaped and concatenated to result in 1D vector fv, i.e., the original feature vector to be transformed. The vector $fv \in \Re^{N'}$, where $N' = 24 \times M \times N$ is the total number of features.

C. Template Transformation With RDM

Initially, the original feature vector fv is multiplied by a large constant, say $c = 100$ due to its low dynamic range. To increase the entropy of the template, fv is salted by ORing it with a random grid RG as $fs = fv + RG$. The random grid RG is user-specific and has the same dimensions as that of fv. RG is generated by assigning random integral values with equal probability in the desired range, e.g., [1 to 255]. Now salted vector is divided into two equal parts $fX = fs(1 : N'/2)$ and $fY = fs(N'/2 + 1 : N')$. Feature point FP_j is defined as $(x_j = fX(j), y_j = fY(j))$ for $j = 1..N'/2$. A user-specific key $\mathcal{K}$ of dimension $1 \times N'$ is generated, which has randomly distributed non-integral values in the range $[-100, 100]$. The key $\mathcal{K}$ is also divided into two equal parts $\mathcal{K}_0$ and $\mathcal{K}_1$ to define mapping for the random point RP_j, $(x_j = \mathcal{K}_0(j), y_j = \mathcal{K}_1(j))$. The distance d_j between the feature points FP_j and random points RP_j are calculated and stored as a new set of features $D = \{d_j\}$, for $1 \le j \le N'/2$ obtained from the original feature vector fv. The process is illustrated in Fig. 2. The computation of random distance is a linear operation. In order to provide non-invertibility, median filtering is applied on distance vector D to generate transformed feature vector Tf, where the intensity values are shuffled in $p \times 1$ neighborhood. Tf is stored as the final transformed template. Transformation keys RG and $\mathcal{K}$ are provided to the user in a tokenized format. The approach also reduces feature dimension by 50%. New transformed template can be generated by changing the transformation keys.

To generate multimodal cancelable templates, the salted features of two modalities (fs_1 and fs_2) are used to form the abscissa and ordinate of features points, i.e., $fX = fs_1$ and $fY = fs_2$. The user-specific key $\mathcal{K}$ of dimensions $1 \times 2N'$ is generated and divided into two equal parts to form the keys $\mathcal{K}_0$ and $\mathcal{K}_1$ for specifying random points. Finally, the distances between the feature points and random points are calculated and shuffled using median filters to form the transformed template. At every authentication, the users' biometric(s) is transformed using the same vectors.

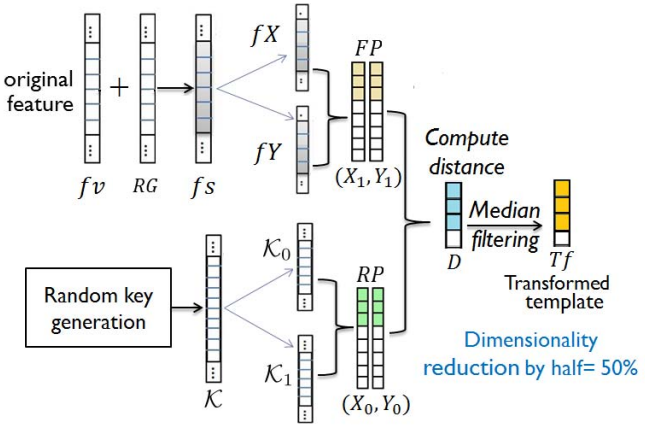

Fig. 2. Template transformation with RDM.

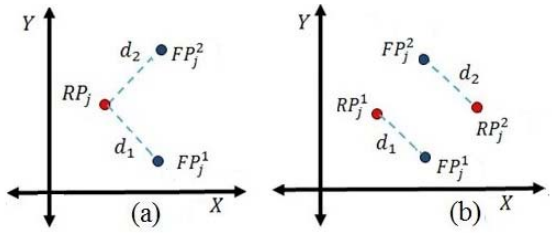

Fig. 3. Ambiguous cases (a) worst-case and (b) best-case scenario.

IV. Some Relevant Issues and Illustrations

A. Ambiguous Cases

The RDM concept believes that the distances of feature points with different random points are different and thereby, can be used for generating revocable features. However, it may give rise to certain ambiguous conditions, where the distance between features points and random points of different user may tend to be same. Consider, the worst-case scenario (Fig. 3(a)), when the same random point RP_j is assigned to all users. There is a possibility that distances d_1 and d_2 between a random point (RP_j) and feature points (FP_j^1 and FP_j^2) belonging to two different users may tend to be same. Similar ambiguity may arise in the best-case scenario (Fig. 3(b)), when each user is assigned a different random point. Here also, distances d_1 and d_2 may tend to be the same. But, this is the case for a single point for some $j \in [1, N'/2]$. For the transformed templates arising from two different features to be same, such cases must come true for more than 60-75% of points. The image samples used for experimentation are of size 128×128. After subjecting it to log-Gabor filters, the size N' of concatenated feature becomes $24 \times 128 \times 128 = 3,93,216$. Therefore, 60% of $N'/2$ accounts approximately 1,17,965, which is a large number for distances to be same

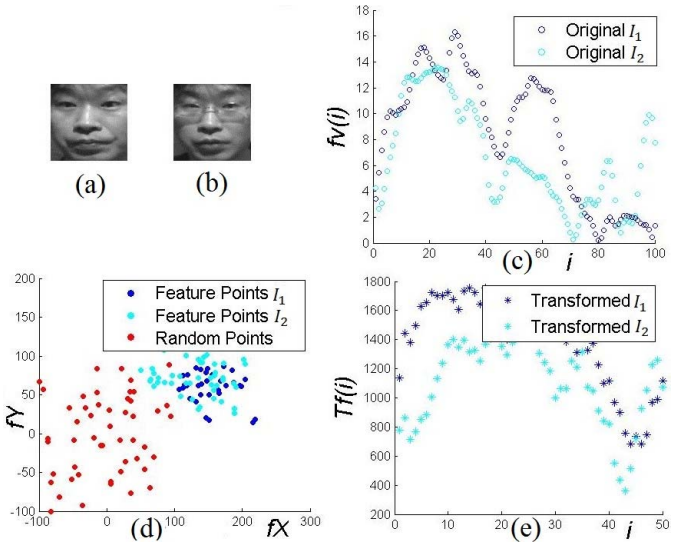

Fig. 4. Point-set distributions illustrating intra-user variations for CASIA face database (a)-(b) sample images I_1 and I_2, (c) original features, (d) feature points and random points, and (e) transformed features.

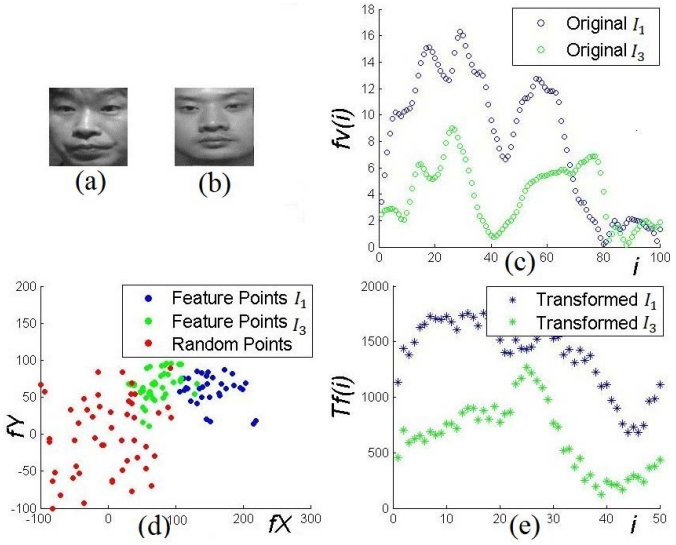

Fig. 5. Point-set distributions illustrating inter-user variations for CASIA face database (a)-(b) sample images I_1 and I_3, (c) original features, (d) feature points and random points, and (e) transformed features.

for features belonging to two users. The proposed approach is experimentally verified for the occurrence of such ambiguities by changing the key $\mathcal{K}$ to generate a number of transformed templates in both worst and best-case scenarios.

B. Point-Set Distribution in the Original and Transformed Domain

For a good scheme, transformed features must preserve intra and inter-user variations. RDM considers features as points in the Cartesian space, the point-set distributions of original and transformed templates generated using the same transformation parameters RG and $\mathcal{K}$ (worst-case scenario) are plotted to visualize the mapping from original to transformed domain and shown in Fig. 4 and 5 for biometric samples belonging to the same and different subjects from CASIA face database. For each image, the first 100 log-Gabor features obtained at $n = 1$ scale and $m = 1$ orientation are mapped as points. Fig. 4(e) depicts the location vs intensity plot for transformed features Tf obtained from the two sample images I_1 and I_2 of the same subject using the same key $\mathcal{K}$. Fig. 5(e) depicts the graph plotted through similar way for transformed features obtained from two different subjects. Along with increased entropy, preservation of intra and inter-user variations in the transformed domain can be observed.

V. Experimental Results and Analysis

Table I provides details of the databases of various modalities used for experimentation. Multimodal databases are also constructed by establishing a one-to-one correspondence between templates belonging to the first $\mathcal{N}$ subjects.

A. Performance Evaluation

As the proposed method must preserve the discriminative information content after transformation, it is expected that the matching performance in the transformed domain should not decrease as compared to the original domain. Matching experiments are also performed with two most prominent feature transformation techniques, namely, 2D BioHash with vector translation [5] and 2D BioPhasor with adaptive thresholding [38] as these techniques are compatible with Gabor based filters. Also, the applicability of these approaches can be generalized for various modalities. BioHashing is implemented for its two variants, BH and BH-50, whereby means of random projection dimensionality of the transformed features is reduced by 50% in BH-50. There is no provision for dimensionality reduction for BioPhasor. The transformed templates are generated using these techniques for the same original features so that the distortion affect can be compared for these approaches and the proposed RDM approach at the same scale.

TABLE I
Databases Used for Experimentation

Modality	Database	Subjects	Samples /subject	k-fold
Face	CASIA-Face V5 (32)	500	5	5
	IRIS(33)	29	10	5
Thermal Face	CASIA NIR(34)	197	10	5
	IRIS(LWIR)(33)	29	10	5
Palmprint	CASIA Palmprint (35)	500	8	4
	CASIA-MS V1(WHT)(36)	200	6	6
Palmvein	CASIA-MS V1(940)(36)	200	6	6
Fingervein	SDUMLA-HMT (37)	636	6	6

1) Evaluation Methods: The system is tuned for k-fold cross validation. For each fold the experiment is repeated 10 times, each time with a different value of user-specific random data. The k-value for each database is reported in Table I. Later, classification and matching is performed using Kernel Discriminant Analysis (KDA) and cosine distances. KDA uses a polynomial based kernel function, which defines a non-linear mapping such that features can be separable and the most significant discriminating information can be extracted [39].

TABLE II

MATCHING PERFORMANCE (*EER%*) FOR ORIGINAL AND TRANSFORMED TEMPLATES IN THE WORST-CASE SCENARIO AT 95% SIGNIFICANCE LEVEL

Reduction	Modality →	Face		Thermal Face		Palmprint		Palmvein	Fingervein
	Scheme↓	CASIA V5	IRIS	CASIA NIR	IRIS(LWIR)	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
-	Original	2.17 ± 0.99	2.06 ± 1.14	0.40 ± 0.21	0.72 ± 0.29	0.50 ± 0.15	1.00 ± 0.55	0.98 ± 0.56	1.10 ± 0.73
	BH	3.30 ± 1.12	3.56 ± 0.98	0.63 ± 0.11	1.39 ± 0.55	0.56 ± 0.23	0.60 ± 0.45	1.25 ± 0.33	1.40 ± 0.25
	BioPhasor	3.50 ± 1.19	10.34 ± 2.16	1.37 ± 0.27	4.41 ± 1.75	1.36 ± 0.41	1.30 ± 0.21	2.00 ± 0.54	2.27 ± 0.54
50%	RDM	2.60 ± 0.97	2.68 ± 1.17	0.80 ± 0.23	0.96 ± 0.56	0.53 ± 0.21	0.60 ± 0.45	0.99 ± 0.21	1.19 ± 0.53
	BH-50	4.52 ± 1.39	3.62 ± 1.00	0.89 ± 0.14	2.05 ± 0.61	0.65 ± 0.15	0.70 ± 0.46	1.50 ± 0.21	1.70 ± 0.21

TABLE III

MATCHING PERFORMANCE (*RI%*) FOR ORIGINAL AND TRANSFORMED TEMPLATES IN THE WORST-CASE SCENARIO AT 95% SIGNIFICANCE LEVEL

Reduction	Modality →	Face		Thermal Face		Palmprint		Palmvein	Fingervein
	Scheme↓	CASIA V5	IRIS	CASIA NIR	IRIS(LWIR)	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
-	Original	92.10 ± 2.24	97.58 ± 1.84	99.64 ± 0.23	99.65 ± 0.23	99.42 ± 0.11	98.60 ± 0.29	98.90 ± 0.21	98.39 ± 1.76
	BH	83.89 ± 3.65	92.41 ± 2.08	99.08 ± 0.07	97.24 ± 0.25	99.34 ± 0.37	98.40 ± 0.96	98.25 ± 0.26	97.48 ± 0.65
	BioPhasor	79.20 ± 3.24	68.96 ± 5.25	96.01 ± 0.93	87.24 ± 1.51	98.88 ± 0.62	97.10 ± 0.87	96.50 ± 0.51	95.47 ± 1.25
50%	RDM	85.88 ± 3.14	94.48 ± 2.98	99.13 ± 0.17	99.35 ± 0.21	99.33 ± 0.16	98.59 ± 0.78	98.60 ± 0.22	98.30 ± 0.53
	BH-50	73.88 ± 2.87	91.37 ± 2.17	98.87 ± 0.21	95.51 ± 1.54	98.68 ± 1.54	98.20 ± 0.82	98.25 ± 0.15	96.30 ± 1.25

TABLE IV

MATCHING PERFORMANCE (*DI*) FOR ORIGINAL AND TRANSFORMED TEMPLATES AT 95% SIGNIFICANCE LEVEL

	Modality →	Face		Thermal Face		Palmprint		Palmvein	Fingervein
Reduction	Scheme ↓	CASIA V5	IRIS	CASIA NIR	IRIS(LWIR)	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
worst-case scenario									
-	Original	4.188 ± 1.390	4.542 ± 0.386	8.765 ± 0.457	4.946 ± 0.209	9.876 ± 1.211	5.970 ± 0.79	6.635 ± 0.112	7.657 ± 1.768
	BH	3.442 ± 1.231	4.464 ± 0.350	6.328 ± 0.472	6.454 ± 0.306	9.851 ± 1.760	5.820 ± 0.325	5.979 ± 0.214	7.314 ± 0.385
	BioPhasor	3.351 ± 1.212	2.672 ± 0.242	5.325 ± 0.221	3.857 ± 0.305	7.692 ± 1.157	5.040 ± 0.273	5.117 ± 0.256	6.050 ± 1.250
50%	RDM	3.860 ± 1.041	4.244 ± 0.264	7.358 ± 0.481	4.629 ± 0.214	9.736 ± 1.340	6.684 ± 0.318	5.985 ± 0.213	7.474 ± 1.542
	BH-50	3.074 ± 1.241	4.320 ± 0.293	6.213 ± 0.121	5.783 ± 0.251	9.621 ± 1.201	5.685 ± 0.287	5.841 ± 0.314	7.101 ± 1.054
best-case scenario									
50%	RDM	23.842 ± 1.21	18.638 ± 1.410	22.0433 ± 1.09	19.908 ± 1.034	19.527 ± 1.035	19.051 ± 1.054	19.934 ± 1.360	18.951 ± 1.980

False Accept Rate (FAR) and False Reject Rate (FRR) are basic performance measures for matching process [40]. These are closely related and defined by the system threshold. FAR and FRR are computed using the scores of genuine and impostor population distribution. *Equal Error Rate* (EER) is defined as a point where FAR and FRR will be equal. The lower the EER, the better the system performance. Another parameter *Decidability Index* (DI) measures the separability of genuine and imposter distributions [40], [41]. Higher DI indicates better separability between genuine and imposter populations resulting in lower false accept and reject rates. Given the genuine and impostor score distribution, DI is calculated using means and standard deviations of genuine (μ_g, σ_g) and imposter (μ_i, σ_g) scores as, $DI = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 + \sigma_i^2)/2}}$.

For verification mode the performance is reported in terms of EER and DI, supported by Receiver Operating Characteristics (ROC) curves. Identification rate at rank-r represents the proportion of identification transactions by a user enrolled in the system, for which user's true identifier is included in the candidate list returned. For identification mode, the performance is reported in terms of Recognition Index (RI) which is identification rate at rank-1 and supported by Cumulative Matching Characteristics (CMC) curves.

2) Evaluation Scenarios: Templates used for experimentation are resized to 128×128 pixels. Neighborhood for median filtering is randomly chosen between [3, 7] for each experiment. Transformed templates are generated for worst-case and best-case scenario to analyze discriminability property.

3) Worst-Case Scenario: To evaluate the distance-preserving property, transformed templates are generated by assigning the same key variables, i.e., RG and $\mathcal{K}$ in the worst-case (stolen key scenario). As the same random points are used for computing distances from all biometric samples, the performance in this scenario helps in exploring discriminability preservation property of RDM. Tables II, III, and IV report matching performance in terms of EER, RI, and DI respectively for the original and transformed unimodal templates at the significance level of 95%. The matching results obtained for the proposed method in the worst-case scenario are slightly less, but comparable to the results obtained with the original templates. The obtained DI values indicate that the transformed templates generated using RDM preserve discriminability to the extent that genuine and impostor populations can be easily separable in the transformed domain. It is found that the verification performance (EER and DI) of the proposed RDM approach (at 50% dimensionality reduction) is mostly better than BH (at no dimensionality reduction) and greater than BH-50 (at 50% dimensionality reduction). In identification scenario, the performance (RI) of RDM is observed to be comparable to BH and better than BH-50. As compared to BioPhasor, the performance of the proposed approach is better for both verification and identification. Table V reports the performance for multimodal transformed

TABLE V

MATCHING PERFORMANCE *EER%*, *DI*, AND *RI%* FOR MULTIMODAL TRANSFORMED TEMPLATES AT 95% SIGNIFICANCE LEVEL

Modalities →	Palmprint+Palmvein	Palmvein+Fingervein	Face+Palmvein	Face+NIR face	Face+LIR face
databases→ parameters↓	CASIA-MS(WHT) + CASIA-MS(940)	CASIA-MS(940) + SDUMLA-HMT	CASIA-Face V5 + CASIA-MS(940)	CASIA-Face V5 + CASIA NIR	IRIS visible + IRIS (LWIR)
EER (worst-case)	0.39 ± 0.20	0.60 ± 0.21	0.60 ± 0.11	0.71 ± 0.34	0.34 ± 0.28
RI (worst-case)	99.20 ± 0.51	99.40 ± 0.24	99.10 ± 0.65	98.78 ± 0.68	99.65 ± 0.41
DI (worst-case)	7.464 ± 0.491	8.091 ± 0.150	7.851 ± 0.714	7.677 ± 0.682	4.951 ± 0.084
DI (best-case)	26.145 ± 0.321	28.875 ± 0.214	27.364 ± 1.244	29.210 ± 0.214	28.113 ± 0.102

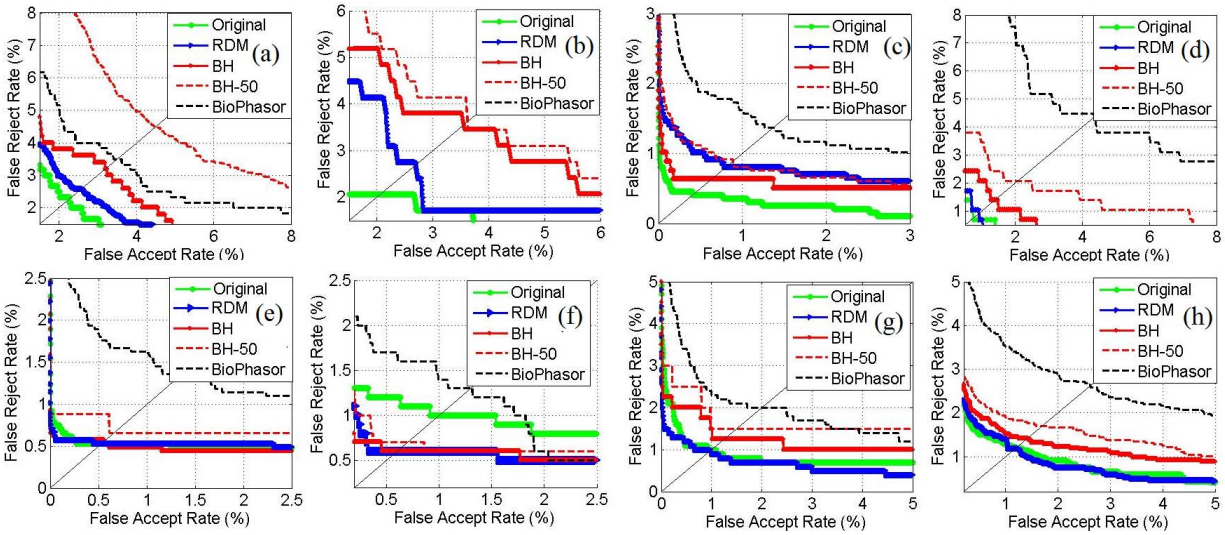

Fig. 6. ROC curves in the worst-case scenario (a) CASIA V5, (b) IRIS, (c) CASIA NIR, (d) IRIS (LWIR), (e) CASIA, (f) CASIA-MS(WHT), (g) CASIA-MS(940), and (h) SDUMLA-HMT.

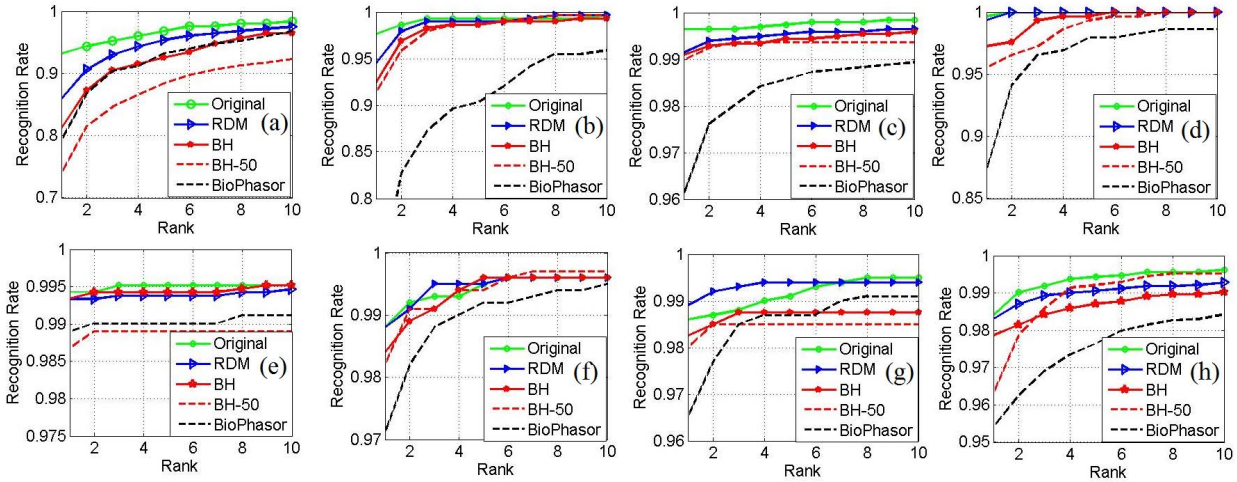

Fig. 7. CMC curves in the worst-case scenario (a) CASIA V5, (b) IRIS, (c) CASIA NIR, (d) IRIS (LWIR), (e) CASIA, (f) CASIA-MS(WHT), (g) CASIA-MS(940nm), and (h) SDUMLA-HMT.

templates generated from the combination of various biometric modalities. With reduced EER, and higher DI and RI, the results indicate an increase in the performance. Thus the proposed RDM approach is found useful for generating unimodal and multimodal cancelable templates. The ROC and CMC curves supporting these results are shown in Fig. 6-8.

4) Best-Case Scenario: In the best case, different key variables are assigned to each user in the database. Experimentally it is found that the random distances computed between different users and random points significantly enhance inter-user variations as very low EER values ($< 0.1E-10$) along with very high $DI (> 18)$ and RI ($> 99.\overline{99}$) values are achieved for all modalities in the best-case scenario. DI values for unimodal and multimodal transformed templates using proposed RDM approach are given in Table IV and V respectively. High DI values support the clear separation between genuine and impostor populations verifying the low error rates obtained in this case. Thus unimodal as well as

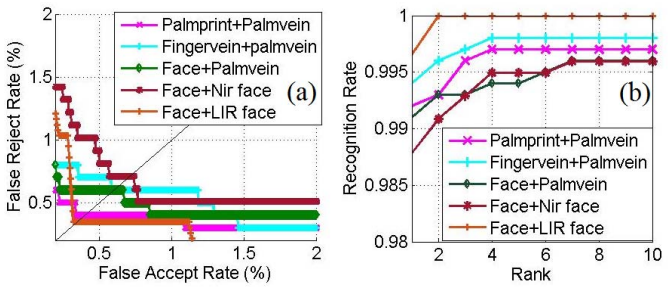

Fig. 8. (a) ROC and (b) CMC curves for multimodal transformed templates.

multimodal transformed templates generated in the best-case scenario using the proposed RDM approach perform better than the original templates.

B. Unlinkability Analysis

Transformed templates generated from the same biometric instance by using different set of user-specific data must be unlinkable. The protocol defined in [30] is used as the benchmark to evaluate unlinkability. To determine unlinkability, a number of transformed template are generated by using different keys which are cross-matched to model *mated* and *non-mated* samples score distributions. *Mated pairs* samples correspond to transformed templates belonging to the same subject generated using different keys, whereas *non-mated pairs* are transformed templates arising from different subjects generated using different keys. For an unlinkable system, there must exist a significant overlap between mated and non-mated score distributions. Two measures are specified by using these distributions: i) $D_{\leftrightarrow}(s)$, which is a local score-wise measure depending upon on the likelihood ratio between score distributions; and ii) $D_{\overleftrightarrow{sys}}$, a global measure, independent of the score domain. These two metrics enable the quantitative assessment of templates unlinkability. $D_{\leftrightarrow}(s) \in [0, 1]$ evaluates the linkability of a system for each specific linkage score s and is defined over the entire score domain. $D_{\leftrightarrow}(s) = 0$ denotes full unlinkability, while $D_{\leftrightarrow}(s) = 1$ denotes full linkability of two transformed templates at score s. However, it is required to estimate the overall unlinkability of the whole system (and not just on a score-wise basis). To have a fairer benchmark, an estimation of the global linkability of a system is calculated using $D_{\overleftrightarrow{sys}} \in [0, 1]$. It is defined that for a system to be unlinkable, all the mated and non-mated samples distribution must overlap for score domain and the global measure $D_{\overleftrightarrow{sys}}$ must be close to zero.

Six transformed databases are generated corresponding to a biometric database by using different user-specific parameters. *Mated* samples score distribution (samples belonging to the same subject transformed using different key) as well as *non-mated pairs* samples score distribution (samples belonging to different subject transformed using different key) are computed across these six databases. These score distributions are used to compute local measure $D_{\leftrightarrow}(s)$, which is further used to compute the overall linkability of the system $D_{\overleftrightarrow{sys}}$. Fig. 9 shows unlinkability curves when transformed templates are generated using CASIA-face V5, CASIA palmprint, SDUMLA-HMT fingervein, and CASIA MS(WHT+940) multimodal databases. With significant overlap, the overall linkability of the system is close to zero for these databases. Similar results are observed for other databases also. Based on this discussion, the proposed system can be considered as unlinkable.

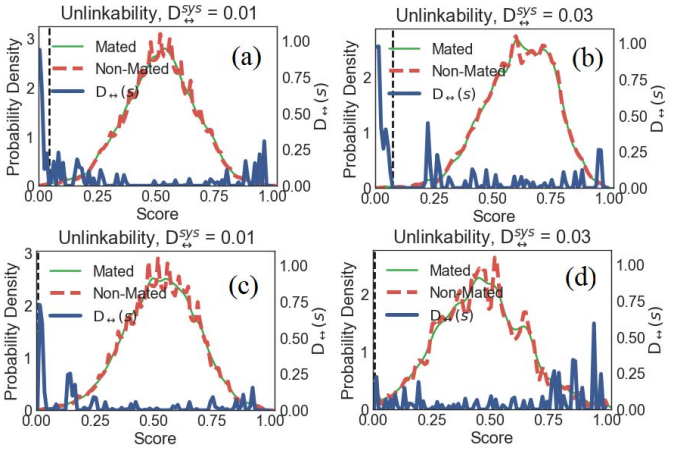

Fig. 9. Unlinkability curves (a) CASIA-face V5, (b) CASIA palmprint, (c) SDUMLA-HMT fingervein, and (d) CASIA MS(WHT+940) multimodal.

C. Non-Invertibility Analysis

The transformed template Tf should be non-invertible even if the user-specific data RG and key $\mathcal{K}$ are simultaneously known to an attacker. The affect of median filtering on random distances is analyzed here to evaluate non-invertibility property of transformed templates. Consider Fig. 10(a) and (b) showing the original feature template fv and random key $\mathcal{K}$. For better visualization, a face image is taken instead of a feature vector. Salting operation is skipped and random distances D are computed between the original features fv and key $\mathcal{K}$ and visualized in Fig. 10(c). Finally, median filtering in small neighborhood ($p = 5$) is applied on D to get transformed template Tf as shown in Fig. 10(d). To check non-invertibility of RDM, inverse operation is simulated on random distances features D as well as stored reference template Tf obtained from D as discussed here.

Case (I) (D and $\mathcal{K}$ Are Known): The random distance matrix D between original feature point FP and random point RP is known. Attacker also knows random point RP (obtained using key $\mathcal{K}$). Now, The attacker may determine the locus of point as a constant distance D from RP. The locus, which is a circle, can then be interpolated at various positions to determine the feature point FP. To simulate the inverse attack, slope $\mathtt{m}$ and intercept $\mathtt{c}$ of the line l joining the feature point $FP(x_p, y_p)$ with random point $RP(x_0, y_0)$ are obtained. As the feature point lies on line $l : y = \mathtt{m}x + \mathtt{c}$ and the random distances are known, the following two equations can be established

$$y_p = \mathtt{m}x_p + \mathtt{c}, \tag{1}$$

and

$$(x_p - x_0)^2 + (y_p - y_0)^2 = d^2, \tag{2}$$

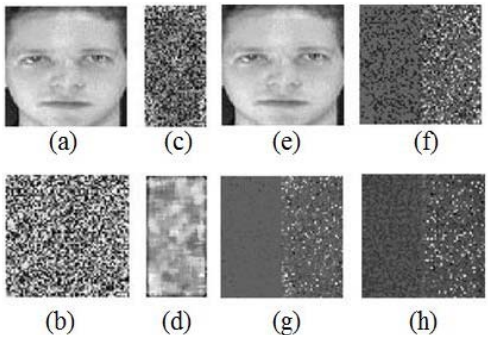

Fig. 10. Non-invertibility analysis using inverse operations (a) original feature fv, (b) key $\mathcal{K}$, (c) distance matrix D, (d) filtered distance matrix Tf, (e) and (f) recovered templates in Case (I), and (g) and (h) recovered templates in Case (II).

where $d \in D$ is the distance between the two points. The above two equations are solved to determine x_p, y_p. Due to quadratic nature, there exists two roots, one being the original feature value and the other is the point opposite to FP at the same distance d from RP. Fig. 10(e) and (f) show the two recovered values. It can be observed from Fig. 10(e) that the original features are recovered.

Case (II) (Tf and $\mathcal{K}$ Are Known): When median filtering is applied to the random distances, then attacker knows Tf. Assuming that slope ($\mathtt{m}$) and intercept ($\mathtt{c}$) of the line joining points are known, the inverse operations are applied and equations 1 and 2 are again solved to obtain x_p, y_p. The solutions obtained in this case as depicted in Fig. 10(g) and (h) are noisy, and do not reveal the original features. This is because median filtering iteratively reshuffles the original distance in its neighborhood and the exact distance is not revealed even if the transformed template is compromised. This justifies the non-invertibility using median filtering over random distance to generate transformed templates.

D. Dictionary Attack

In dictionary attack, the attacker maps every possible point in the original space to the transformed one by using leaked transformed template, key, and transformation function [42]. This set of mapped points (called as dictionary) are used to build a pre-image in the original domain. As the transformed template (Tf) is the distance value, here the mapping is to be defined for all possible feature points (x, y) to distance values which results when the other set of random points (defined by transformation key) are known. The dictionary consists of entries $((x, y), P, Tf{=}\mathrm{RDM}((x,y),P))$ for all possible (x, y) in the original Cartesian space, where P is the set of transformation parameters and RDM is the proposed transformation function. The set of parameters P consists of multiplication constant c, salting values RG, random key points $\mathcal{K}$, and median filtering neighborhood p in the entire transformation process. This way the entire transformation $((x, y) \rightarrow Tf)$ consists of four intermediate mapping functions $f_1 \ldots f_4$. Thus the attacker has to build all possible pairs $((x, y), f_1((x, y),\mathrm{c}), f_2(f_1, RG), f_3(f_2, \mathcal{K}), f_4(f_3, p))$. Also, the attacker must have an approximate intensity range of original features to execute this process, which may vary depending upon the modality, subject, and feature extraction technique. Even though one has some idea of this intensity range and he is able to establish the first three functions, but the last transformation, i.e., median filtering makes the entire effort in vain as it iteratively shuffles the transformed value at i^{th} location with the median value in its p neighborhood.

The above discussion is illustrated with the help of an example. Let the original feature $fv \in [0, 10]$ and defined as $fv = [7.5, 6.5, 5.0, 5.5, 3.0, 7.5, 2.0, 7.0, 2.0, 4.0, 3.5, 4.0, 0.5, 5.0, 4.0, 2.5, 2.5, 2.5, 2.0, 3.0]$. For simplifying illustration c is considered as 1 and salting operation using RG is skipped. This gives $fX = [7.5, 6.5, 5.0, 5.5, 3.0, 7.5, 2.0, 7.0, 2.0, 4.0]$ and $fY = [3.5, 4.0, 0.5, 5.0, 4.0, 2.5, 2.5, 2.5, 2.0, 3.0]$ to form feature points. Let $\mathcal{K}_0, \mathcal{K}_1 \in$[-10,10] and these random points are defined as $\mathcal{K}_0 = [0, 6.5, 6, 3, -2.5, 6.5, 0.5, -3, 9, 7.5]$ and $\mathcal{K}_1 = [1, 2.5, 2, -6, -4, -0.5, -5.5, 7, -6.5, -5.5]$. The distance vector $D = [7.91, 1.50, 1.80, 11.28, 9.71, 3.16, 8.14, 10.97, 11.01, 9.20]$. Median filtering in $p = 5$ neighborhood on D gives $Tf = [1.50, 1.80, 7.91, 3.16, 8.14, 9.71, 9.71, 9.20, 9.20, 9.20]$. It can be observed that not only values are shuffled, but some values are repeated. Now let the Tf and parameters $\mathcal{K}$, $c = 1$ and $p = 5$, and intensity range for original features [0,10] be known to the attacker. Then the dictionary building process is shown in Fig. 11. Initially, the attacker builds a mapping of all possible feature points in [0,10], say at a step interval of 0.5 (Fig. 11(a)) resulting in a dictionary $Dict$ with 400 entries. Then using the knowledge of key ($\mathcal{K}_0$, $\mathcal{K}_1$), all possible combinations of feature points with random points are defined (Fig. 11(b)) resulting in 4000 entries, from which all possible distances are determined (Fig. 11(c)). Finally, using Tf, $\mathcal{K}_0$, $\mathcal{K}_1$, and these mappings, one to one correspondence is established to determine the original features. It can be seen in Fig. 11(d) that for distance defined by $Tf(3)$ there can be more than one pre-image mappings arising from different key combinations. Thus for each distance value, various attempts are required to map pre-image. However, this process will not be effective as the correct intensity location for which the values corresponds to Tf is not known. The attacker cannot identify that $Tf(3)$ is resulting from $D(1)$ even if p is known. Further, Tf is overwritten at many intensity locations, from which the correct D values cannot be known. Thus, determining only intensity mapping is not enough as the original pre-image heavily depends upon the location of intensity values. In this example Tf consists only 10 entries, but the actual size of Tf is large, i.e., $(24 \times 128 \times 128)/2 = 1,96,608$ here. Use of salting operations will further result in manifold increase in dictionary size. Building a dictionary for the pre-image attack seems to be non-feasible when shuffling is performed over such a large set of values.

E. Attacks via Record Multiplicity

In attacks via record multiplicity (ARM), the attacker gets access to more than one copy of transformed templates obtained from the same instance and attempts to link them in

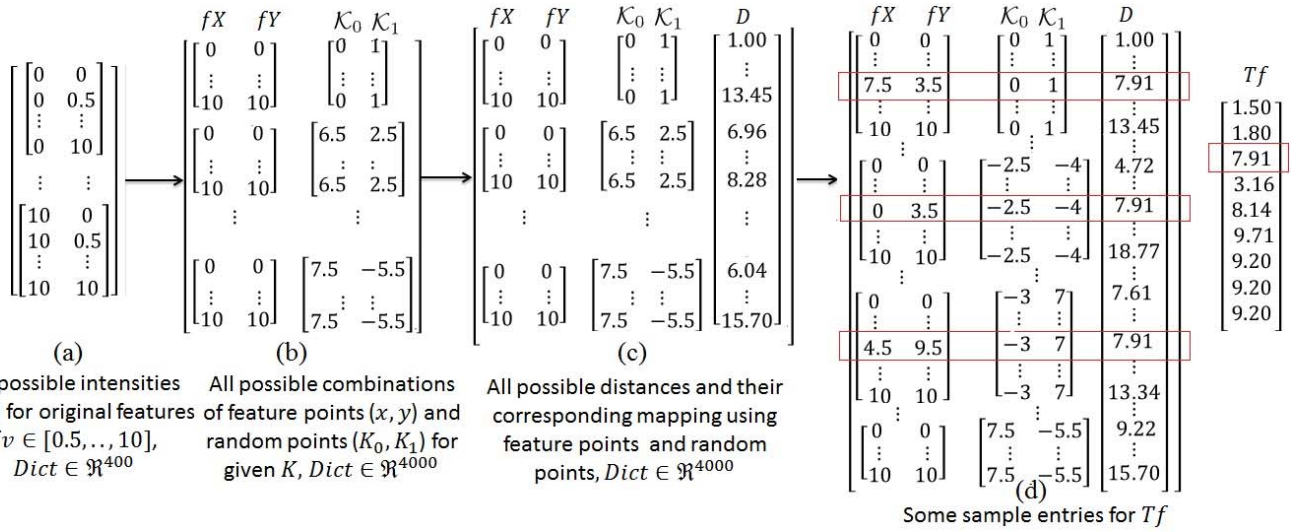

Fig. 11. Step-wise construction of dictionary.

order to build a possible pre-image of the original template. Let Tf_1 and Tf_2 be two transformed templates generated from the same biometric instance, but by using different parameters, say $P_1 = (c_1, RG_1, \mathcal{K}_1, p_1)$ and $P_2 = (c_2, RG_2, \mathcal{K}_2, p_2)$ respectively. It is already shown experimentally that these templates are unlinkable. Further, the i^{th} location of Tf_1 depends upon the distance vector D_1 and its shuffling neighborhood p_1. It cannot be linked to i^{th} location of Tf_2 as it depends upon the sequence of its distance vector D_2 and shuffling neighborhood p_2. The intensities of these distance vectors would vary due to change in salting parameters and random points. Further, it is not feasible to recover D_1 and/or D_2 by knowing Tf_1 and/or Tf_2 in light of the discussions presented for unlinkability, non-invertibility, and dictionary attack. Therefore, multiple copies of the transformed templates are seemed to be not useful for an adversary to perform ARM.

F. False Accept Attack

It is also a kind of dictionary attack where an attacker having appropriate knowledge of transformation algorithm and parameters uses some publicly available benchmark databases to masquerade the system. Here, the attacker subjects the biometric samples of a public database to transformation algorithm using known parameters in order to generate a wide set of transformed templates. These pseudo-transformed templates are then inputted to the system for gaining illegitimate access. The attack is simulated as follows. Initially, original transformed templates are generated for the first database, say DB_1 having 'K'users, such that each user is assigned a different set of parameters. Also, a set of pseudo-transformed templates is generated using second database, say DB_2 having 'P' users, such that for each user transformed templates are generated using all 'K' different parameters used for the first database. The training samples of DB_1 are crossed matched with the pseudo-transformed templates of DB_2 to determine systems false accept rate. Table VI reports the results when cross matching is performed. FAR close to zero indicating resistance of the proposed approach towards false accept attack.

TABLE VI
FALSE ACCEPT ATTACK ANALYSIS

DB_1	Subjects	DB_2	Subjects	EER
CASIA-Face V5	500	IRIS	29	0.0000%
CASIA NIR	197	IRIS(LWIR)	29	0.0001%
IRIS(LWIR)	29	IRIS	29	0.0000%
CASIA-MS V1(WHT)	200	CASIA Palmprint	500	0.0939%

G. Brute Force Attack

Here the attacker does not have any information about the original template or the transformation keys. He tries all possible permutations and combinations to generate a transformed template and make a successful attempt. For an image of 128×128, the transformed template size is 1,96,608 and it consists of distance values $\in [0, \infty]$ whose range depends upon the transformation parameters. Transformed templates are bounded by a maximum value of 2000 (see Fig. 5) for parameters defined in this work. This amounts to a brute force effort of the order 196608^{2000}, which is very high.

VI. CONCLUSION

The proposed approach is simple and easy to implement. Transformed templates generated using RDM are experimentally verified and compared with the original and other transformation techniques for various modalities. With 50% reduced dimension, unimodal transformed templates are found to deliver good matching performance even in the worst-case scenario. Multimodal transformed templates are also found to give good matching performance for different combinations of biometric modalities. Other important requirements like revocability, unlinkability, and non-invertibility are also satisfied.

REFERENCES

[1] N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: A case study in fingerprints," in *Proc. 18th Int. Conf. Pattern Recognit.*, vol. 4, Aug. 2006, pp. 370–373.
[2] A. T. B. Jin, D. N. C. Ling, and A. Goh, "BioHashing: Two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, Apr. 2004.

[3] P. Lacharme, E. Cherrier, and C. Rosenberger, "Preimage attack on BioHashing," in *Proc. Int. Conf. Secur. Cryptogr.*, Jul. 2013, pp. 1–8.
[4] A. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 37, no. 5, pp. 1096–1106, Oct. 2007.
[5] Y. Wang and K. N. Plataniotis, "An analysis of random projection for changeable and privacy-preserving biometric verification," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 40, no. 5, pp. 1280–1293, Oct. 2010.
[6] R. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognit.*, vol. 40, no. 3, pp. 1057–1065, Mar. 2007.
[7] Y. Kim and K.-A. Toh, "A method to enhance face biometric security," in *Proc. Int. Conf. Biometrics, Theory, Appl., Syst.*, Sep. 2007, pp. 1–6.
[8] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," in *Proc. Int. Conf. Acoust., Speech Signal Process.*, Mar. 2010, pp. 1838–1841.
[9] M. Savvides, B. V. K. V. Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proc. 17th Int. Conf. Pattern Recognit. (ICPR)*, vol. 3, 2004, pp. 922–925.
[10] E. Maiorana, P. Campisi, and A. Neri, "Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system," in *Proc. IEEE Int. Syst. Conf.*, Apr. 2011, pp. 495–500.
[11] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognit.*, vol. 47, no. 3, pp. 1321–1329, 2014.
[12] A. B. Teoh and D. C. Ngo, "Biophasor: Token supplemented cancellable biometrics," in *Proc. 9th Int. Conf. Control, Automat., Robot. Vis.*, Dec. 2006, pp. 1–5.
[13] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancelable iris biometric," in *Proc. 19th Int. Conf. Pattern Recognit.*, Dec. 2008, pp. 1–4.
[14] F. Quan, S. Fei, C. Anni, and Z. Feifei, "Cracking cancelable fingerprint template of Ratha," in *Proc. Int. Symp. Comput. Sci. Comput. Technol.*, vol. 2, Dec. 2008, pp. 572–575.
[15] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2007, pp. 1–7.
[16] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 236–246, 2010.
[17] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable fingerprint templates with delaunay triangle-based local structures," in *Cyberspace Safety and Security*. Cham, Switzerland: Springer, 2013, pp. 81–91.
[18] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia Pairs," *Pattern Recognit.*, vol. 66, pp. 295–301, Jun. 2017.
[19] R. Dwivedi, S. Dey, R. Singh, and A. Prasad, "A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping," *Comput. Secur.*, vol. 65, pp. 373–386, Mar. 2017.
[20] Y.-L. Lai *et al.*, "Cancellable iris template generation based on indexing-first-one hashing," *Pattern Recognit.*, vol. 64, pp. 105–117, Apr. 2017.
[21] Z. Jin, J. Y. Hwang, Y.-L. Lai, S. Kim, and A. B. J. Teoh, "Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 393–407, Feb. 2018.
[22] L. Nanni and A. Lumini, "Empirical tests on BioHashing," *Neurocomputing*, vol. 69, nos. 16–18, pp. 2390–2395, Oct. 2006.
[23] A. M. de Paula Canuto, M. C. Fairhurst, and F. Pintro, "Ensemble systems and cancellable transformations for multibiometric-based identification," *IET Biometrics*, vol. 3, no. 1, pp. 29–40, Mar. 2013.
[24] P. P. Paul and M. Gavrilova, "Multimodal cancelable biometrics," in *Proc. IEEE 11th Int. Conf. Cogn. Inform. Cogn. Comput.*, Aug. 2012, pp. 43–49.
[25] P. P. Paul and M. L. Gavrilova, "A novel cross folding algorithm for multimodal cancelable biometrics," *Int. J. Softw. Sci. Comput. Intell.*, vol. 4, no. 3, pp. 20–37, 2012.
[26] P. P. Paul, M. Gavrilova, and S. Klimenko, "Situation awareness of cancelable biometric system," *Vis. Comput.*, vol. 30, no. 9, pp. 1059–1067, 2013.
[27] C. Rathgeb and C. Busch, "Cancelable multi-biometrics: Mixing iris-codes based on adaptive bloom filters," *Comput. Secur.*, vol. 42, pp. 1–12, May 2014.
[28] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and K. O. M. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion," *Inf. Fusion*, vol. 18, pp. 161–174, Jul. 2014.
[29] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, "Multi-biometric template protection based on bloom filters," *Inf. Fusion*, vol. 42, pp. 37–50, Jul. 2018.
[30] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 6, pp. 1406–1420, Jun. 2018.
[31] H. Kaur and P. Khanna, "Cancelable features using log-Gabor filters for biometric authentication," *Multimedia Tools Appl.*, vol. 76, no. 4, pp. 4673–4694, 2016.
[32] CASIA-FaceV5. *Biometrics Ideal Test,*. [Online]. Available: http://biometrics.idealtest.org
[33] University Tennessee. *IRIS Thermal/Visible Face Database*. [Online]. Available: http://www.cse.ohio-state.edu/otcbvs-bench
[34] S. Z. Li, R. Chu, S. Liao, and L. Zhang, "Illumination invariant face recognition using near-infrared images," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 627–639, Apr. 2007.
[35] *CASIA Palmprint Database, Biometrics Ideal Test*. [Online]. Available: http://biometrics.idealtest.org/downloadDB/
[36] *CASIA-MS-Palmprint V1, Biometrics Ideal Test*. [Online]. Available: http://biometrics.idealtest.org
[37] Y. Yin, L. Liu, and X. Sun, "SDUMLA-HMT: A multimodal biometric database," in *Biometric Recognition*. Berlin, Germany: Springer, 2011, pp. 260–268.
[38] L. Leng and J. Zhang, "PalmHash code vs. PalmPhasor code," *Neurocomputing*, vol. 108, pp. 1–12, May 2013.
[39] M.-H. Yang, "Kernel Eigenfaces vs. Kernel Fisherfaces: Face recognition using kernel methods," in *Proc. 5th IEEE Int. Conf. Autom. Face Gesture Recognit.*, vol. 2, May 2002, pp. 215–220.
[40] R. M. Bolle, S. Pankanti, and N. K. Ratha, "Evaluation techniques for biometrics-based authentication systems (FRR)," in *Proc. 15th Int. Conf. Pattern Recognit.*, vol. 2, Sep. 2000, pp. 831–837.
[41] G. O. Williams, "The use of d' as a 'decidability' index," in *Proc. 30th Annu. Int. Conf. Secur. Technol.*, Oct. 1996, pp. 65–71.
[42] S. W. Shin, M.-K. Lee, D. Moon, and K. Moon, "Dictionary attack on functional transform-based cancelable fingerprint templates," *ETRI J.*, vol. 31, no. 5, pp. 628–630, 2009.

Harkeerat Kaur has completed Ph.D. in CSE (2018), PDPM IIITDM, Jabalpur, India. Her research interests include image processing, biometrics, and cryptography.

Pritee Khanna is currently an Associate Professor with CSE, PDPM IIITDM, Jabalpur, India. Her research interests include biometrics, content-based image retrieval, human–computer interaction, and medical image processing.