Polynomial Transformations to Generate Cancelable Biometric Features with Reduced Dimensions

Harkeerat Kaur and Pritee Khanna

***Abstract*—Cancelable biometrics is a template protection technique which is proposed to bridge the growing gap between '*biometrics for security*' and '*security for biometrics*'. Various approaches have been reported in literature, yet transforming a biometric template is a challenging task. A novel polynomial based template transformation technique is proposed in this work to generate protected templates named as 'PolyCodes'. These protected versions are privacy preserving, revocable, and provide significant dimensionality reduction. Several polynomial functions with dimensionality reduction factor ranging from 65% to 90% are designed and evaluated for security and performance. Further, applicability of the proposed 'PolyCodes' is experimentally verified for many biometric modalities such as visible and thermal face, palmprint, palmvein, and fingervein.**

***Index Terms*—Biometrics, Cancelable, Log-Gabor filter, Non-invertibility, Polynomial transformation**

I. Introduction

Biometrics is a modern world authentication technology where access is granted on the basis of an individual's biological and behavioral characteristics. In spite of many advantages such as higher security and ease of use, advances in biometrics authentication technology have given rise to numerous security and privacy concerns. With advancement in technology, illegal accesses using biometric identities have been reported to increase (1). The templates stored as digital entities in the database accessed over LAN or remote web server are most vulnerable to hacking and other malicious activities. The present day concern is the risk of losing biometric identities and its ramifications. Unlike passwords, biometric identity cannot be renewed on compromise. Loss of biometric identity at some common and less secure application may affect the effectiveness of its usage at some security critical application also.

Various template protection schemes are proposed to bridge the growing gap between 'biometrics for security' and 'security for biometrics'. Cancelable biometric is a template protection approach that uses token-supplemented user-specific secret information (key/parameter) to generate pseudo-biometric identities that retain important discriminative information and can be used for authentication purposes. These pseudo-identities can be easily regenerated and do not reveal any information about the original biometrics. This way cancelable biometrics provides high level privacy, security, and revocability to biometrics that may help to increase information privacy and public confidence.

A framework for biometric authentication is proposed in this work which uses polynomial based transformation functions to generate cancelable biometric features. The transformed features named as 'PolyCodes' here, fulfill template protection requirements and also provide significant dimensionality reduction ranging from 65% to 90%. Extensive experiments are performed on multiple modalities to showcase effectiveness of the proposed technique.

The work is organized as follows. Section II provides insight to cancelable biometric and discusses existing template transformation techniques. The concept of random polynomial based feature transformation is presented in Section III and generation of 'PolyCodes'is discussed in Section IV. Performance analysis of 'PolyCodes' for non-invertibility, revocability, and diversity properties is performed in Section V and finally, the work is concluded in Section VI.

H. Kaur and P. Khanna are with the Department of Computer Science and Engineering, PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur, India, e-mail: (pkhanna@iiitdmj.ac.in).

II. Cancelable Biometrics and Literature Review

Cancelable template proposed by Ratha et al. (2001) (2) is a transformed version of original biometric template which is generated by using some user-specific auxiliary data. The basic cancelable biometric setup is shown in Fig. 1. At enrollment, the original biometric identity (M) of a user is transformed with the help of some secret key/auxiliary data to generate a transformed feature/pseudo-biometric identity (PI) which is stored as a reference template. At authentication, the probe biometric (M') of the same user is transformed in the similar way to generate transformed query template (PI'). Transformed Reference and query templates are matched to determine access. Cancelable biometric transformation must fulfill four essential properties: *non-invertibility*, *discriminability*, *revocability*, and *diversity* (3). *Non-invertibility* enhances security, while *discriminability* ensures that the essence of biometric data is maintained. In case of attack, only pseudo-biometric identity (PI) is compromised, which can be regenerated by changing transformation function and/or keys (*revocability*) (4). Different pseudo-identities can be generated from the same biometric for diverse usage across different applications (*diversity*). This provides unlinkability to databases and takes care of cross-matching problem.

Template transformation schemes are broadly classified as *biometric salting* and *non-invertible transforms*. Biometric salting techniques are further classified as *Random Projection*, *Random Convolution*, and *Random Noise* based transforms. The techniques under these categories are discussed below.

Random Projection (RP) based transformations are most widely used biometric salting techniques. RP transforms biometric data by projecting it over a random sub-space defined by user-specific key. Teoh et al. (2004) proposed the most popular biometric salting technique known as BioHashing (5).

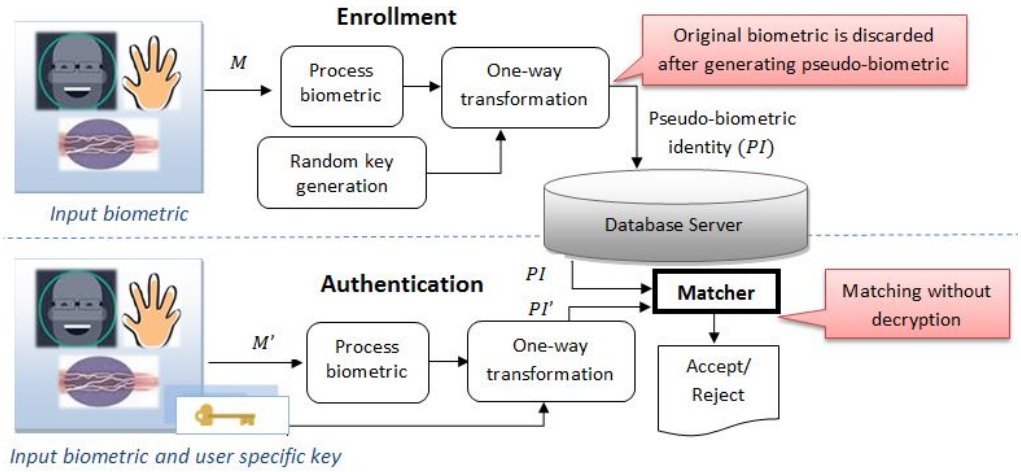

Fig. 1. Enrollment and authentication processes with cancelable biometrics.

Here, the biometric features are salted by projecting them on random subspace defined by orthonormal random matrices. It is later quantized into binary codes via thresholding operations to achieve many-to-one mapping and ensuring non-invertibility. Although the approach is well known to preserves discriminability, it is also susceptible to inverse operations if the transformed biometric and projection matrix are leaked (6). Various techniques such as Random Mutlispace Quantization (RMQ) in BioHash (7), Multi-space Random Projections (MRP) (8), User-dependent Multi-state Discretization (Ud-MsD) BioHash (9), RP with vector translation (10) are proposed to improve upon the drawbacks.

Random Convolution based transformations convolve biometric signal with some random kernel to generate transformed templates. Savvides et al. (2004) transformed face images by convolving them with random kernels (11). However, de-convolution can be attempted to recover features if random kernel is known. Maiorana et al. (2010) proposed BioConvolving, which uses random user-specific key to divide the original feature into fixed sized segments that are later convolved to generate transformed templates (12). However, discriminability and non-invertibility properties are not justified in stolen token scenario. Wang et al. (2014) used curtailed circular convolution in which binary fingerprints features are convolved with random binary strings in circular manner to impart non-invertibility (13).

Random Noise based transformations distort biometric templates by adding random noise patterns. Teoh et al. (2006) proposed BioPhasoring to generate a set of complex vectors where the original features form real part and the user-specific random vectors form imaginary part (14). The phase/arctangent of the complex vector is used as non-invertible transformed template. Leng et al. (2013) improvised BioHashing and BioPhasoring techniques for palmprint modality (15). The transformation algorithm is extended to 2D for both the techniques to generate templates with reduced computational complexity and storage cost. Zuo et al. (2008) proposed GRAY salting (template based salty noise) and BIN salting (code based salty noise) for generating cancelable iris templates (16). These techniques add unique random noise or synthetic textures to underlying Gabor features. Kaur and Khanna (2016) XORed original features with random patterns that is followed by median filtering to ensure non-invertibility (17).

Non-invertible transforms map biometric features to a new random subspace such that the inverse mapping is not possible. Ratha et al. (2007) proposed three functions that randomly map fingerprint minutiae points to a new subspace using Cartesian, polar, and surface folding transforms (4). Inspite of many-to-one mappings used by these transform, Quan et al. (2008) proved that the transforms are invertible when transformed templates and parameters are simultaneously known (18). Similarly, Farooq et al. (2007) and Lee and Kim (2010) proposed a many-to-one mapping of minutiae features onto a predefined 3D array based on some user-specific key and reference minutia's position and orientation (19; 20). However, the mapping used here tends to compromise discriminability. Also inverse attacks are possible if user specific key are revealed. Yang et al. (2013) (21) extracted local structures of minutiae features using Delaunay triangulation which were subjected to non-invertible polar transformation. Wang et al. (2017) used partial discrete Fourier transform to get good performance as the local structures of minutiae points preserve discriminability after non-invertible distortions (22). Dwivedi et al. (2016) proposed randomized look-up table mapping to generate cancelable iris templates (23). Consistent bits are extracted from features to generate randomly mapped decimal value. But the mapping can be inverted, if look-up table and transformation parameters are known. Another scheme proposed by Jin et al. (2017) maps real-valued iris features into discrete index (max ranked) hashed codes. It is based on locality sensitive hashing (LSH) also known as 'Index-of-Max (IoM)' hashing (24). Cho and Wang (2017) proposed random permutation maxout transform, which maps a real-valued face feature vector into a discrete index code that is used as a transformed template (25).

Development of revocable, discriminability preserving, and non-invertible cancelable templates is a challenging task especially when transformation function, key, and/or transformed template are simultaneously known. Various data hiding and secret sharing schemes use polynomials and its variants for

providing information security (26; 27). Also, many polynomial based fuzzy vault and fuzzy commitment schemes exist under cryptosystem category (28; 29). However, these techniques do not provide strong biometric privacy as the original biometric can be recovered from the protected template (30; 31; 32). The technique proposed in this work explores the use of polynomial functions for generating *non-invertible* and *discriminability* preserving cancelable biometric features with *reduced dimensionality*. The proposed polynomial function takes a set of biometric features as coefficients and evaluated at some random points specified by user-specific key to map transformed features. Also a trade-off between dimensionality reduction and discriminability is established by designing and evaluating several polynomial functions to aid flexibility in dimensionality reduction from 65% to 90%.

III. Proposed Random Polynomial Transformation

A polynomial based feature transformation approach is proposed to construct a uni-variable or multi-variable polynomial such that its coefficients are salted biometric features. The polynomial is then evaluated at some random point and the output value is taken as transformed quantity.

At the first step, the original feature vector fv is salted by ORing it with a random grid RG. This initial level salting break the intensity correlation between neighboring features and increase entropy of the template. Random grid RG has the same dimensions as that of fv and is generated by assigning random integral values in the desired range, e.g., [-255 to 255].

$$fs = fv + RG \tag{1}$$

The template transformation function is designed as a polynomial function $f(.)$ in variable μ and degree ν. The total number of possible terms in such a polynomial are $\rho = \begin{pmatrix} \nu+\mu \\ \nu \end{pmatrix}$. The resulting features (fs) are divided into fixed sized non-overlapping blocks of dimension ρ. The total number of blocks in which fs may be divided are $b = N/\rho$ after applying suitable padding operation wherever necessary. Let the features in j^{th} block of fs be referred as $a_i^j = \{a_1^j, a_2^j, ..., a_\rho^j\}$. Depending upon the values of μ and ν, a polynomial function is defined for each j^{th} block, such that feature a_i^j of that block forms the coefficient for the i^{th} term in the polynomial, where $1 \leq i \leq \rho$ and $1 \leq j \leq b$. Thus for a uni-variate polynomial in degree 2 ($\mu = 1$, $\nu = 2$, $\rho = 3$), feature fs is divided into fixed sized blocks of dimension 3 and a polynomial function is constructed corresponding to each block.

$$f(x) = a_1^j + a_2^j x + a_3^j x^2 \tag{2}$$

here $f(x)$ is a polynomial in variable 'x' whose coefficients are salted features a_i^j belonging to a particular block. Also, a user-specific vector X (called evaluation matrix) of dimensions $1 \times b$ having non-integral random values in the range [-100, 100] is generated with a random number generator. For each j^{th} block, the salted features are mapped to some random point using transformation polynomial and evaluation point.

$$Tf(j) = f(X(j)), \tag{3}$$

TABLE I
Some combinations of μ and ν for polynomial construction.

Variables	Degree	Terms ρ	PolyCode-$\mu\nu$	Reduction
Uni-variate, $\mu = 1$	$\nu = 2$	3	PolyCode-12	66.66%
	$\nu = 3$	4	PolyCode-13	75.00%
Bi-variate, $\mu = 2$	$\nu = 2$	6	PolyCode-22	83.33%
	$\nu = 3$	10	PolyCode-23	90.00%
Tri-variate, $\mu = 3$	$\nu = 2$	10	PolyCode-32	90.00%
	$\nu = 3$	20	PolyCode-33	95.00%

where $X(j) \in X$ and $1 \leq j \leq b$. The transformed template Tf is concatenation of the values evaluated for each j^{th} block and is called 'PolyCodes'. Similarly for a bi-variate polynomial in degree 2 ($\mu = 2$, $\nu = 2$), block size ρ will be 6 and the transformation function will be defined as

$$f(x, y) = a_1^j + a_2^j x + a_3^j y + a_4^j xy + a_5^j x^2 + a_6^j y^2 \tag{4}$$

$f(x, y)$ is a bi-variable polynomial and its coefficients are salted features of j^{th} block represented as $a_i^j = \{a_1^j, ..., a_6^j\}$. The transformed features or PolyCodes are evaluated as

$$Tf(j) = f(X(j), Y(j)) \tag{5}$$

here X and Y are user-specific evaluation matrices each of dimension $1 \times b$ having randomly distributed non-integral values in the range [-100, 100]. Similarly for a bi-variate polynomial in degree 3 ($\mu = 2$, $\nu = 3$, $\rho = 10$), the transformation polynomial function is

$$\begin{aligned} f(x, y) = {} & a_1^j + a_2^j x + a_3^j y + a_4^j x^2 + a_5^j y^2 \\ & + a_6^j xy + a_7^j x^2 y + a_8^j xy^2 + a_9^j x^3 + a_{10}^j y^3 \end{aligned} \tag{6}$$

This way multi-variate polynomials can be constructed for different values of μ and ν (Table I). Output transformed features Tf are named as PolyCode-$\mu\nu$ and used for storing and matching purposes. The proposed transformation approach also reduces feature size by a factor d depending upon the dimension of block size, i.e., $d = 1/\rho$.

Fig. 2 depicts a step wise illustration for generation of PolyCodes-12 ($\mu = 1$, $\nu = 2$, $\rho = 3$), PolyCodes-22 ($\mu = 2$, $\nu = 2$, $\rho = 6$), and PolyCodes-32 ($\mu = 3$, $\nu = 2$, $\rho = 10$). Fig. 2(a) shows the distribution of original features belonging to j^{th} block of feature vector fv. Fig. 2(b) shows the distribution of features belonging to the same block after salting operation is performed. Fig. 2(c) depicts the mapping of salted features after polynomial transformation. Corresponding to each block, a transformed value is obtained according to the values in random evaluation matrices, i.e., X in case of PolyCodes-12, (X, Y) for PolyCodes-22, and (X, Y, Z) for PolyCodes-32. As evaluation matrices are user-specific, each user is assigned a different set of random evaluation points and provided to him in a tokenized format. The vector Tf is revocable. A new one can be generated by changing random evaluation matrices and/or random grid in case of a compromise.

However,the range of evaluation matrix, number of variables, and the highest degree of the polynomial must be controlled in order to maintain the performance. Due to exponential nature of the transform, increase in degree may tend to increase the weight of some feature components in

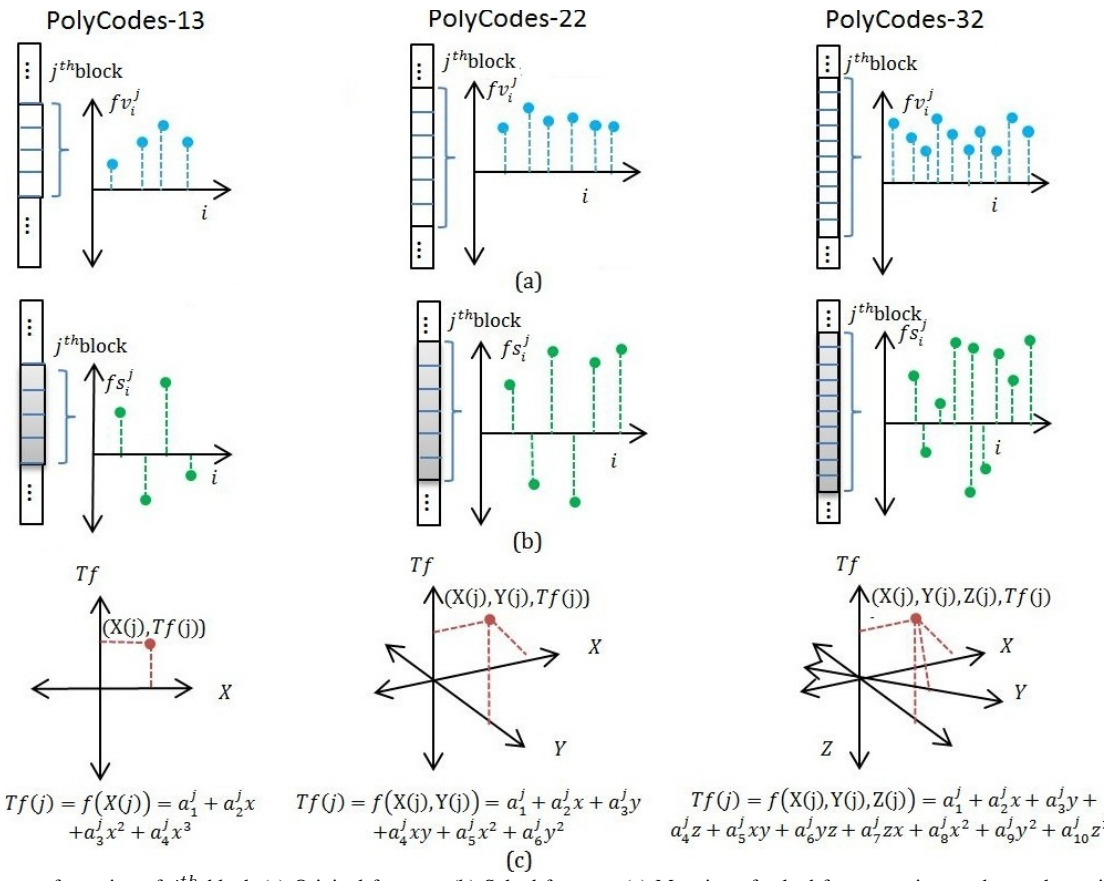

Fig. 2. Feature transformation of j^{th} block (a) Original features, (b) Salted features, (c) Mapping of salted features using random polynomial method.

the polynomial. This may increase burst errors and affect the overall discriminability of features. Increase in the value of μ and ν tends to affect discriminability and will also increase the complexity of the transform. Revocability and non-invertibility issues are discussed in later sections.

IV. Generating PolyCodes

Feature extraction using log-Gabor filters: The proposed work uses log-Gabor filter to extract features from biometric images belonging to different modalities at multiple space and frequency resolutions (33). Log-Gabor filters are evolved versions of Gabor filters that offer better spectral coverage and handle rotational variations. It captures local spatial frequencies and statistics of images in a better way as compared to Gabor and other wavelet filters. Log-Gabor filters are defined as Gaussian transfer functions over logarithmic frequency scale which are composed of radial (r) and angular components (θ) defined in polar coordinate system as

$$G(r,\theta) = exp\left(\frac{log(r/f_0)}{2\sigma_r^2}\right).exp\left(\frac{-(\theta-\theta_0)^2}{2\sigma_\theta^2}\right) \quad (7)$$

where (r,θ) represents polar coordinates and 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 $f_0 = 1/minWave \times mult^n$. In this work, the 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 $6 \times 4 = 24$ filters. The values assigned to the parameters are $\sigma_r = 0.55$, $\sigma_\theta = 1.5$, $mult = 3$, and $minWave = 3$ (33).

Let I be a biometric signal image of dimensions $M \times N$ is preprocessed for noise removal and extraction of ROI. The responses at multiple resolutions are calculated by multiplying Fast Fourier Transform (FFT) of image with filter response at different scales (n) and orientations (m). The final output is a complex value from which magnitude patterns are computed. For $n = 4$ scales and $m = 6$ orientations, the obtained pattern is vector $fv_{m,n}$ of size $M \times N$. The vector $fv_{m,n}$ is reshaped to 1D which forms the original feature vector to be transformed.

Feature transformation using random polynomial method: As the magnitude patterns have low dynamic range, initially the original feature vector is multiplied by large constant $c = 100$. range. At the first step, OR operation is performed using RG and salted features are obtained $fs_{m,n}$. For each combination of μ and ν, salted vector is divided into non-overlapping block of dimension ρ, using which polynomial function is constructed. It is evaluated at the given user-specific evaluation matrix to generate the transformed features $Tf_{m,n}$. The transformed template is a concatenation of transformed features obtained at each scale and resolution known as PolyCodes-12, PolyCodes-13, PolyCodes-22, PolyCodes-23, PolyCodes-32, and PolyCodes-33 depending upon univariable, bi-variable, and tri-variable based polynomial.

Point-Set Distribution in the Original and Transformed Domain: For a good scheme, the transformed features must

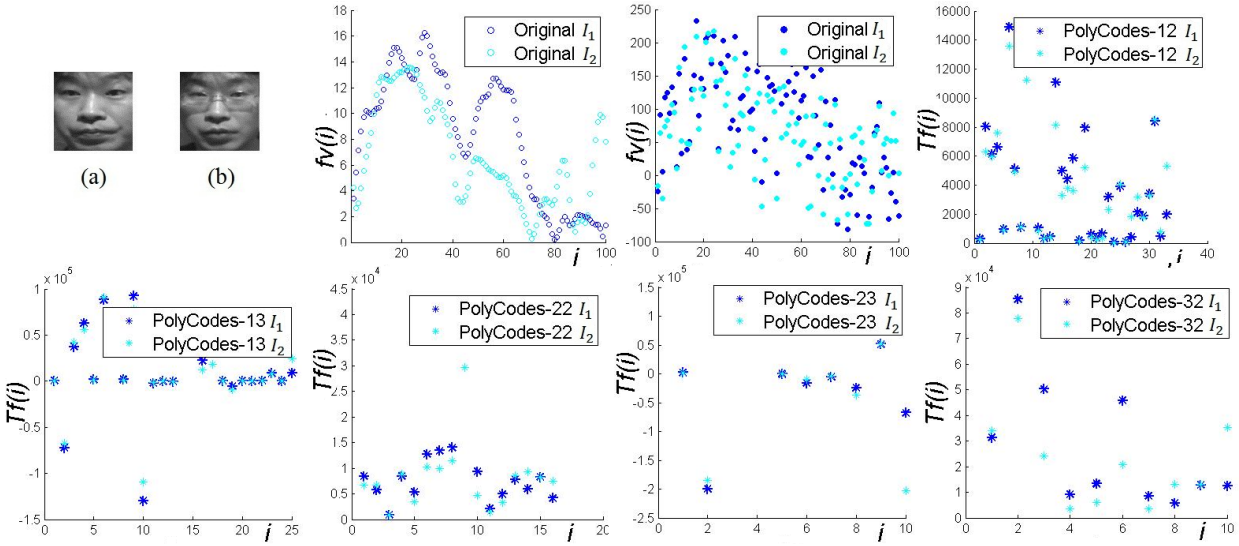

Fig. 3. Point-set distributions illustrating intra-user variations for CASIA face (a)-(b) sample images I_1 and I_2, (b) original features, (c) salted features; transformed features (d) PolyCodes-12, (e) PolyCodes-13, (f) PolyCodes-22, (g) PolyCodes-23, and (h) PolyCodes-32.

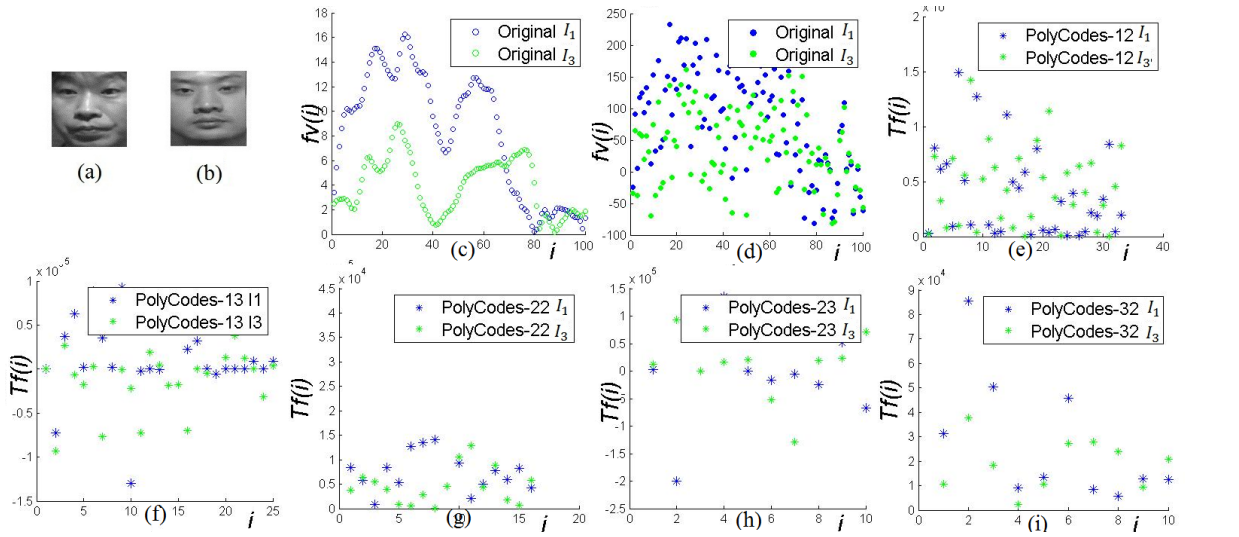

Fig. 4. Point-set distributions illustrating inter-user variations for CASIA face (a)-(b) sample images I_1 and I_3, (b) original features, (c) salted features; transformed features (d) PolyCodes-12, (e) PolyCodes-13, (f) PolyCodes-22, (g) PolyCodes-23, and (h) PolyCodes-32.

preserve intra and inter-user variations. The point-set distributions of original and transformed templates, generated using same transformation parameters, random grid RG and evaluation matrices (X/Y/Z) (*worst-case scenario*), are plotted to visualize the mapping from original to transformed domain. Fig. 3 and 4 illustrate examples of the point-set distribution for original, salted, and transformed features corresponding to biometric samples belonging to the same and different subjects from CASIA face database. Fig. 3(a) and (b) show two original biometric face images I_1 and I_2 belonging to the same subject. For each image, features are extracted using log-Gabor transform. The scatter graphs are plotted with spatial location 'i' on the x-axis and its corresponding intensity values on the y-axis for the first 100 feature vectors obtained with log-Gabor filter at $n = 1$ scale and $m = 1$ orientation. The original, salted, and transformed features for different PolyCodes are shown in the Fig. 3(e)-(f). Here, an increase in randomness can be observed. Also, the transformed features exhibit similar patterns indicating preservation of intra-user variations. Similarly, Fig. 4(a)-(b) depict sample face images I_1 and I_3 of two different subjects and the mapping of their original, salted features, and transformed features obtained using the same parameters RG and (X/Y/Z) in Fig. 4(e)-(f) respectively. Along with the increased entropy, the preservation of inter-user variations in transformed domain can be also observed.

V. Experimental Results and Analysis

The proposed approach is experimentally analyzed for various properties on multiple modalities. The databases used for experimentation are summarized in Table II.

A. Performance Evaluation

***Evaluation Methods*:** The system is tuned for k-fold cross validation, where k-1 folds are used for training and the remaining fold is used for testing. 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 II. 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 for feature vectors that exhibit significant variations such that features can be separable and the most significant discriminating information can be extracted (34).

False Accept Rate (FAR) and False Reject Rate (FRR) are basic measures of matching performance. They are closely related and defined by the system threshold. Another index, *Equal Error Rate* (EER) is a point where FAR and FRR are equal. The lower the EER, the better the system performance. Another useful parameter *Decidability Index* (DI) measures the separability of genuine and imposter classes. DI is defined as the normalized distance between the means of genuine (μ_g) and imposter (μ_i) distributions (35). It measures the confidence in classifying patterns for a given classifier. Higher DI indicates better decidability while classifying genuine and imposter populations. DI is calculated as

$$DI = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 + \sigma_i^2)/2}} \tag{8}$$

For verification mode the performance is reported in terms of EER and DI, which are 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 are supported by Cumulative Matching Characteristics (CMC) curves.

***Comparison Techniques*:** The matching performance must be preserved when the system operates using transformed templates. In order to establish a baseline for comparison, matching performance is calculated using original templates (fv). It is expected that the transformed templates must preserve the essence of biometric information and their matching performance should not decrease much as compared to original templates. Comparisons are also performed using four prominent techniques belonging to different feature transformation categories namely, Random Projection with vector translation (Wang et al., 2010 (10)), BioConvolving (Maiorana et al., 2010 (12)), 2D BioPhasor with adaptive thresholding (Leng et al., 2013 (15)), and Random Maxout Permutation Transform (Cho and Wang, 2017 (25)). Random Projection with vector translation is implemented for its three variants namely- RPv, RPv-50 and RPv-75, where by means of random projection the dimensionality of transformed features is reduced by 50% in RPv-50 and 75% in RPv-75. For BioPhasor and BioConvolving there are no provision of dimensionality reduction. BioConvolving and Random Permutation Maxout (RPM) transform are implemented according to their best parameter definitions described in (12; 25). The transformed templates are generated using these techniques using same original log-Gabor features (fv) so that the distortion affect can be compared on same scale.

TABLE II
DATABASES USED FOR EXPERIMENTATION.

Modality	Database	Subjects	Samples/subject	k-fold
Face	CASIA-Face V5 (36)	500	5	5
	ORL (37)	40	10	5
Thermal Face	CASIA NIR(38)	197	10	5
	IRIS (39)	39	10	5
Palmprint	CASIA Palmprint (40)	301	8	4
	CASIA-MS V1 (WHT) (41)	200	6	6
Palmvein	CASIA-MS V1 (940) (41)	200	6	6
Fingervein	SDUMLA-HMT (42)	636	6	6

***Evaluation Scenarios*:** All image templates used for experimentation are resized to 80×80 pixels, which are subjected to feature extraction and transformation under the under worst-case as well as best-case scenarios.

***Worst-case or stolen-token scenario*:** Here the security of the system is checked when an attacker is always in possession of users' secret keys. The situation assumes that the secret key is always public and checks for the discriminability of the transform. To ensure that the discriminative information content is not harmed and the proposed transform is effective, each biometric sample of the database is transformed using the same user-specific keys, i.e., random grid (RG) and evaluation points ($X/Y/Z$). When same parameters are used, each sample is distorted on the same scale and they are expected to match like original undistorted features. Table III, IV, and V report matching results in terms EER, RI, and DI at a significance level of 95% for the transformed variants.

It is observed that matching performance using PolyCode-12 is quite comparable to that obtained with the original features. Although matching performance obtained for PolyCode-12 degrades as compared to original features, but it is worth to mention that this small degradation when PolyCode-12 uses only 33.34% features as compared to the 100% features used in the original scheme. This shows that in spite of significant dimension reduction, discriminative information is retained up to a significant level by PolyCode-12. The performance degrades as the variables and degree of polynomial are increased, which is quite obvious. The performance of PolyCodes degrades more with increasing degree of transform polynomial as compared to the increasing number of variables used. EER of PolyCode-13 is greater (i.e., performance degradation) than EER of PolyCode-12. The same is true with PolyCode-22 and PolyCode-23. At the same time, performance of PolyCode-22 (using 17% features) and PolyCode-32 (using 10% features) are very close. The performance of PolyCode-23 falls as the number of terms with higher degree tends to be more. Thus, it can be inferred that for evaluation matrix in the range [-100, 100], the highest degree ν is suggested to be at most 2 with number of variable μ may vary up to 3. Similar trends are observed for DI and RI values. ROC and CMC curves shown in Fig. 5 and Fig. 6 also support these findings.

The performance of PolyCode-12 (at 67% reduction) is less than RPv (at no reduction), however PolyCode-13 (at 75% reduction) better than RPv-50 (at 50% reduction). PolyCode-22 at 83% reduction is better than RPv-50 at 50% reduction for many modalities and better than RPv-75 at 75% reduction. As

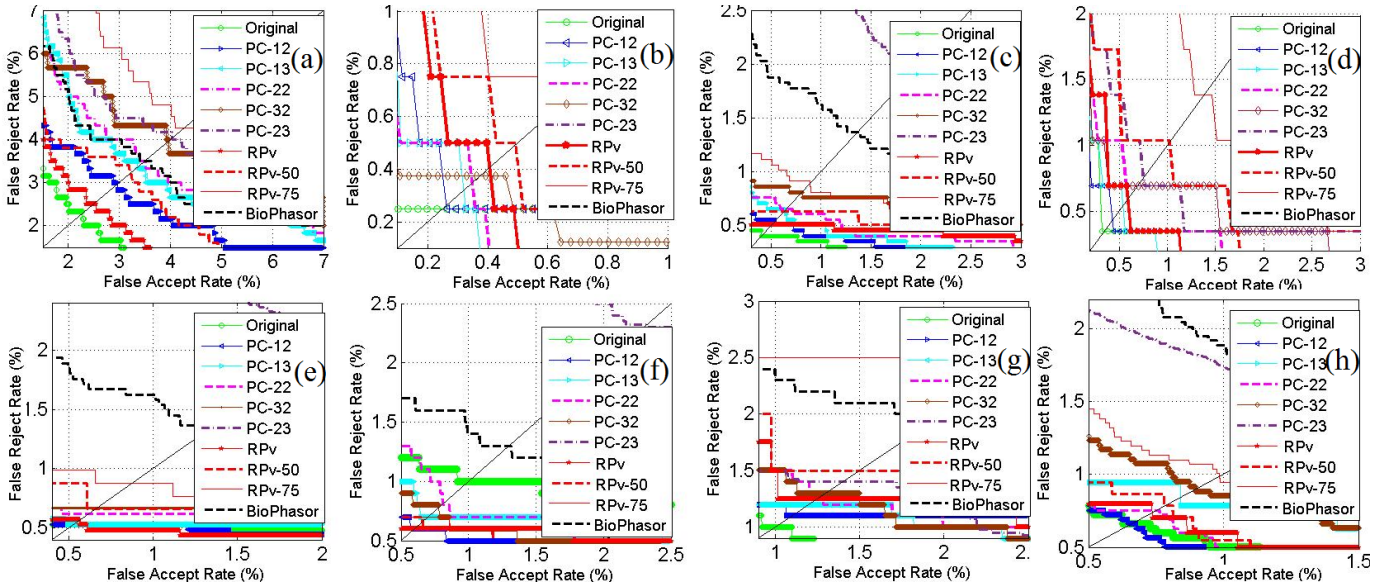

Fig. 5. ROC curves in the worst-case scenario (a) CASIA V5 face, (b) ORL face, (c) CASIA NIR V5 thermal face, (d) IRIS thermal face, (e)CASIA-MS V1 (WHT), (f)CASIA-MS V1 (940nm), (g) CASIA-MS V1 (940nm) palmvein, and (h) SDUMLA-HMT fingervein.

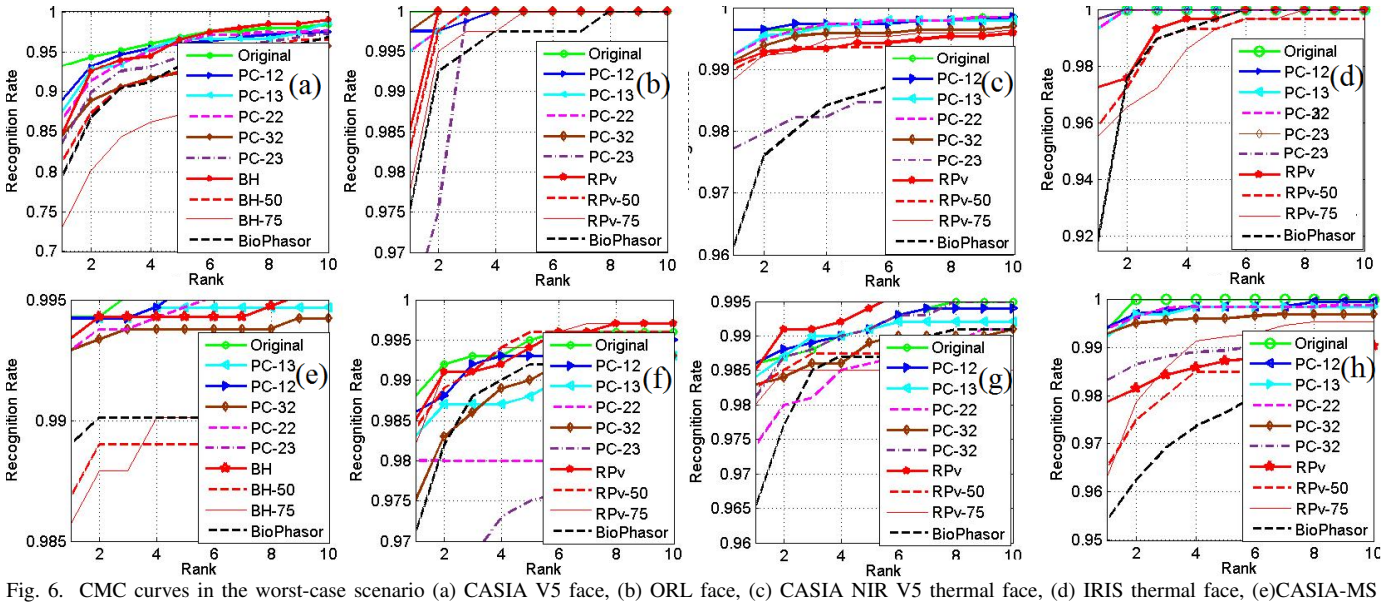

Fig. 6. CMC curves in the worst-case scenario (a) CASIA V5 face, (b) ORL face, (c) CASIA NIR V5 thermal face, (d) IRIS thermal face, (e)CASIA-MS V1 (WHT), (f)CASIA-MS V1 (940nm), (g) CASIA-MS V1 (940nm) palmvein, and (h) SDUMLA-HMT fingervein.

TABLE III

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	ORL	CASIA NIR	IRIS	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
-	Original	2.17 ± 0.99	0.24 ± 0.14	0.40 ± 0.21	0.33 ± 0.12	0.50 ± 0.16	0.99 ± 0.55	1.00 ± 0.56	0.66 ± 0.21
	RPv	2.50 ± 1.12	0.44 ± 0.10	0.50 ± 0.12	0.63 ± 0.27	0.56 ± 0.23	0.60 ± 0.35	1.25 ± 0.36	0.71 ± 0.21
	BioPhasor	3.50 ± 2.19	1.26 ± 0.43	1.37 ± 0.27	4.41 ± 0.21	1.36 ± 0.31	1.30 ± 0.21	2.01 ± 0.31	1.49 ± 0.21
	BioConvolving	7.84 ± 1.07	2.50 ± 0.46	3.80 ± 0.89	7.20 ± 1.15	2.88 ± 0.87	6.00 ± 1.12	5.50 ± 0.95	2.20 ± 0.62
	RPM	9.28 ± 3.08	6.75 ± 2.42	7.30 ± 4.86	13.50 ± 0.18	4.00 ± 1.37	2.83 ± 1.50	4.50 ± 2.38	1.73 ± 0.62
50%	RPv-50	3.30 ± 0.97	0.49 ± 0.13	0.68 ± 0.14	1.02 ± 0.69	0.65 ± 0.31	0.66 ± 0.35	1.50 ± 0.21	0.78 ± 0.32
66.66%	PolyCode-12	2.82 ± 1.63	0.27 ± 0.14	0.54 ± 0.23	0.43 ± 0.11	0.53 ± 0.27	0.60 ± 21	1.10 ± 0.61	0.66 ± 0.24
75%	RPv-75	4.20 ± 1.63	0.75 ± 0.52	0.76 ± 0.21	1.25 ± 0.27	0.88 ± 0.31	0.70 ± 0.46	2.17 ± 0.21	0.97 ± 0.15
	PolyCode-13	3.33 ± 2.11	0.32 ± 0.07	0.65 ± 0.28	0.54 ± 0.21	0.54 ± 0.26	0.69 ± 0.43	1.19 ± 0.52	0.75 ± 0.30
83.33%	PolyCode-22	3.49 ± 2.07	0.35 ± 0.06	0.67 ± 0.29	0.59 ± 0.25	0.62 ± 0.38	0.80 ± 0.25	1.29 ± 0.53	0.81 ± 0.39
90%	PolyCode-23	4.12 ± 2.44	1.62 ± 0.65	2.07 ± 2.09	0.76 ± 0.43	2.08 ± 0.62	2.32 ± 1.92	1.40 ± 0.55	1.42 ± 0.83
	PolyCode-32	3.95 ± 1.51	0.37 ± 0.14	0.81 ± 0.38	0.69 ± 0.21	0.57 ± 0.27	0.78 ± 0.22	1.30 ± 0.75	0.89 ± 0.21

TABLE IV
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	ORL	CASIA NIR	IRIS	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
-	Original	92.10 ± 2.24	100.00 ± 0.00	99.64 ± 0.23	99.65 ± 0.22	99.42 ± 0.31	98.60 ± 0.29	98.60 ± 0.21	99.41 ± 1.76
	RPv	84.89 ± 3.65	98.50 ± 0.21	99.08 ± 0.12	97.24 ± 0.75	99.34 ± 0.37	98.52 ± 0.64	98.50 ± 0.96	97.77 ± 1.25
	BioPhasor	79.20 ± 3.24	97.50 ± 0.75	96.09 ± 0.93	96.09 ± 0.93	98.94 ± 0.62	97.10 ± 1.25	96.50 ± 0.25	95.47 ± 1.36
	BioConvolving	54.80 ± 6.25	97.50 ± 0.85	90.60 ± 1.32	84.84 ± 3.22	90.55 ± 1.25	68.50 ± 5.25	74.00 ± 3.21	90.29 ± 2.22
	RPM	64.88 ± 10.04	96.25 ± 6.61	88.20 ± 4.20	77.24 ± 9.37	95.25 ± 2.24	95.33 ± 1.21	91.60 ± 4.85	95.60 ± 1.67
50%	RPv-50	81.20 ± 2.87	98.25 ± 0.24	98.97 ± 0.75	95.86 ± 2.08	98.68 ± 0.58	98.40 ± 0.23	98.25 ± 0.54	96.50 ± 1.35
66.66%	PolyCode-12	89.13 ± 2.12	99.75 ± 0.21	99.64 ± 0.18	99.65 ± 0.31	99.42 ± 0.27	98.60 ± 1.08	98.30 ± 0.92	99.40 ± 0.21
75%	RPv-75	73.00 ± 3.17	97.76 ± 0.78	98.83 ± 0.25	95.51 ± 1.84	98.57 ± 0.64	98.20 ± 0.31	98.06 ± 0.84	96.39 ± 1.26
	PolyCode-13	87.60 ± 2.43	99.50 ± 0.29	99.23 ± 0.35	99.31 ± 0.61	99.40 ± 0.19	98.30 ± 0.59	98.30 ± 1.08	99.21 ± 0.35
83.33%	PolyCode-22	86.63 ± 2.39	99.50 ± 0.18	99.23 ± 0.38	99.30 ± 0.27	99.29 ± 0.34	98.00 ± 1.08	97.40 ± 0.98	99.37 ± 0.35
90%	PolyCode-23	83.93 ± 2.62	96.20 ± 1.25	97.71 ± 4.83	99.65 ± 0.31	96.17 ± 1.84	95.40 ± 2.01	98.10 ± 0.99	98.30 ± 0.83
	PolyCode-32	84.43 ± 2.65	99.75 ± 0.45	99.13 ± 0.44	99.66 ± 0.61	99.29 ± 0.49	97.50 ± 0.50	98.10 ± 1.50	99.27 ± 0.32

TABLE V
MATCHING PERFORMANCE (*DI*) 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	ORL	CASIA NIR	IRIS	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
-	Original	4.188 ± 1.390	6.436 ± 0.243	8.765 ± 0.457	4.946 ± 0.209	9.876 ± 1.211	5.970 ± 0.791	6.635 ± 0.112	7.657 ± 1.768
	RPv	3.442 ± 1.231	5.699 ± 0.332	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	4.549 ± 0.221	5.325 ± 0.221	3.857 ± 0.305	7.692 ± 1.157	5.040 ± 0.273	5.117 ± 0.256	6.050 ± 1.250
	BioConvolving	2.562 ± 0.114	3.980 ± 0.105	3.551 ± 0.098	2.727 ± 0.110	3.624 ± 0.121	2.628 ± 0.101	2.903 ± 0.083	3.747 ± 0.033
	RPM	2.577 ± 0.385	2.947 ± 0.388	6.097 ± 0.311	2.636 ± 0.424	5.351 ± 1.441	4.065 ± 0.405	3.383 ± 0.601	3.747 ± 0.033
50%	RPv-50	3.074 ± 1.241	5.329 ± 0.332	6.213 ± 0.121	5.783 ± 0.251	9.621 ± 1.201	5.685 ± 0.287	5.841 ± 0.314	7.101 ± 1.054
66.66%	PolyCode-12	4.418 ± 1.321	6.367 ± 0.248	8.663 ± 0.746	4.990 ± 0.073	9.926 ± 1.682	7.253 ± 0.460	6.250 ± 0.760	0.867 ± 0.154
75%	RPv-75	3.010 ± 1.471	5.415 ± 0.183	6.123 ± 0.130	5.521 ± 0.123	9.514 ± 1.191	5.313 ± 0.437	5.436 ± 0.114	6.978 ± 1.124
	PolyCode-13	4.352 ± 1.231	6.363 ± 0.238	8.097 ± 0.581	4.924 ± 0.077	8.476 ± 0.214	5.946 ± 0.275	5.799 ± 0.325	8.450 ± 0.882
83.33%	PolyCode-22	4.308 ± 1.323	6.533 ± 0.231	7.890 ± 0.556	4.960 ± 0.120	8.611 ± 1.374	5.674 ± 0.251	6.051 ± 0.664	8.499 ± 1.452
90%	PolyCode-23	4.278 ± 1.232	3.251 ± 0.215	4.088 ± 0.251	4.891 ± 0.239	5.163 ± 0.421	5.361 ± 0.927	5.540 ± 0.242	6.019 ± 1.474
	PolyCode-32	4.306 ± 1.322	6.314 ± 0.280	7.022 ± 0.609	4.965 ± 0.093	8.649 ± 0.198	5.584 ± 0.551	5.939 ± 0.608	7.892 ± 1.151

TABLE VI
MATCHING PERFORMANCE (*DI*) FOR TRANSFORMED TEMPLATES IN THE BEST-CASE SCENARIO AT 95% SIGNIFICANCE LEVEL.

Modality →	Face		Thermal Face		Palmprint		Palmvein	Fingervein
Scheme↓	CASIA V5	ORL	CASIA NIR	IRIS	CASIA	CASIA-MS	CASIA-MS(940)	SDUMLA-HMT
PolyCode-12	28.244 ± 1.012	28.599 ± 1.321	22.645 ± 1.851	22.414 ± 1.654	27.506 ± 1.325	28.654 ± 1.228	28.484 ± 1.118	21.709 ± 1.258
PolyCode-13	27.504 ± 1.412	26.720 ± 1.021	21.437 ± 1.224	22.119 ± 1.650	26.779 ± 1.021	27.069 ± 1.514	27.170 ± 1.332	21.349 ± 1.162
PolyCode-22	26.592 ± 1.212	26.200 ± 1.541	18.428 ± 1.223	18.534 ± 1.361	25.742 ± 1.202	29.401 ± 1.632	25.390 ± 1.455	20.085 ± 1.362
PolyCode-23	16.512 ± 1.410	14.218 ± 1.541	16.222 ± 1.225	19.173 ± 1.322	19.349 ± 1.313	25.622 ± 1.541	22.548 ± 1.205	18.725 ± 1.021
PolyCode-32	15.761 ± 1.228	15.714 ± 1.332	17.898 ± 1.332	19.304 ± 1.021	19.342 ± 1.210	26.318 ± 1.541	24.473 ± 1.851	19.907 ± 1.724

compared to BioPhasor, the matching performance is clearly better upto PolyCode-22 and mostly better for PolyCodes-32. As compared to BioConvolving and Random Permutation Maxout transform (RPM), the performance of various PolyCodes variants is distinctly higher indicating better discriminability preservation.

***Best-case scenario*:** Matching performance is also evaluated for best-case scenario, when each user in the database is assigned a different set of transformation parameters RG and evaluation matrices $(X/Y/Z)$. Use of different RG for each individual changes the salted features, which in turn changes the coefficients of the polynomial. As different matrices are allotted to each individual, the evaluation points also change. Overall, this leads to tremendous increase in the evaluated values Tf belonging to different individual, thereby resulting in low error rates $EER < 0.01E-10$ and good recognition index $RI > 99.\overline{99}$. The DI values reported in Table VI which are $DI > 18$ indicating high decidability, and further supporting the low error rates obtained. Also, it can be observed that DI values for PolyCodes-12 to PolyCodes-22 are relatively higher as compared to PolyCodes-23 and PolyCodes-32.

B. Unlinkability Analysis

In order to provide good revocability and diversity, the transformed templates generated from the same biometric instance by using different set of user-specific data must be unlinkable. The protocol defined in (43) 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

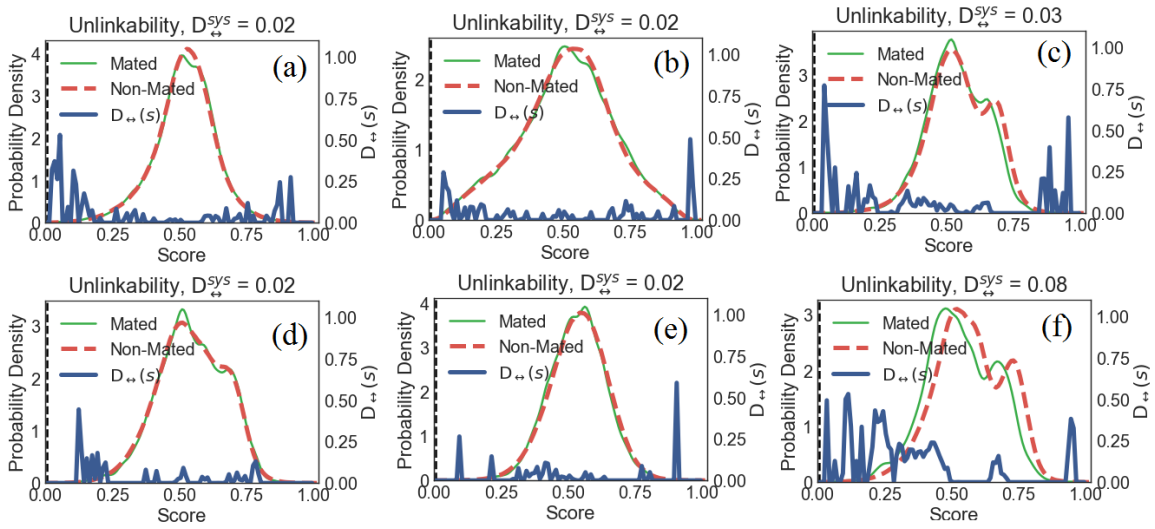

Fig. 7. Unlinkability Curves for CASIA V5 face and CASIA palmprint: (a) and (d) PolyCodes-12, (b) and (e) PolyCodes-23, (c) and (f) PolyCodes-32.

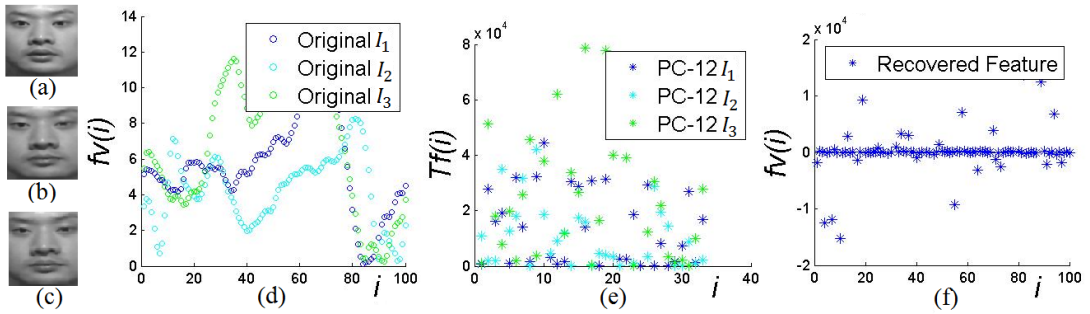

Fig. 8. Point-set distributions illustrating revocability (a)-(c) sample images I_1,I_2 and I_3, (d) original features, (e) transformed features (PolyCodes-12), (f) recovered features from different Polycodes using interpolation method.

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) $D_{\overset{sys}{\leftrightarrow}}$, 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 $D_{\overset{sys}{\leftrightarrow}} \in [0, 1]$. 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 $D_{\overset{sys}{\leftrightarrow}}$ 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 $D_{\overset{sys}{\leftrightarrow}}$. Fig. 7 shows unlinkability curves when transformed templates are generated using CASIA V5 face and CASIA Palmprint database for different PolyCode variants. 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.

C. Attacks-via-Record Multiplicity (ARM)

The security of the proposed approach needs to be checked if an attacker obtains multiple copies of revoked templates. If ρ or more copies of user-specific tokenized variables and revoked templates generated from the same biometric are available, the attacker may formulate it as an interpolation problem and try to solve it to approximate the polynomial coefficients (salted features). Polynomial interpolation for univariate and multi-variate cases is discussed in (44). Different transformed templates can be generated from the same by changing the user specific parameters RG and $(X/Y/Z)$. The attack is simulated here by generating $\rho = 3$ copies of transformed templates corresponding to PolyCodes-12.

Fig. 8(a)-(c) depicts three face images I_1, I_2, and I_3 belonging to the same user. The first 100 features of these images extracted using log-Gabor transform at resolution $m = 1$, $n = 1$ are shown in Fig. 8(d). These features are transformed using different evaluation points to generate different PolyCodes-12

as illustrated in Fig. 8(e). For simplification salting operation is skipped while generating transformed templates. Fig. 8(f) illustrates the point set distributions when one tries to recover the original templates from the three transformed templates by interpolation. Although in such a case one may expect the recovered set to be an approximation of original salted features, but it is actually not so. This is because the sample arising from the same biometric (of a particular user) does not contain exactly the same values, but only similar feature values. This leads to variations in their evaluated values causing interpolation error, which would increase with the use of salting operations. Therefore, multiple copies of the transformed templates are seemed to be not useful for an adversary to perform ARM.

D. Non-invertibility Analysis

The non-invertibility property of the cancelable features requires that even if the user-specific transformation parameters are known, the transformed template should not be invertible to obtain the pre-image of original template. Consider a scenario, when the transformed template and evaluation matrices are simultaneously available to the attacker. The problem of determining the original biometric features from the knowledge of transformed template and evaluation point is same as approximating an unknown function $f(.)$. Determining a polynomial function $f(.)$ from the knowledge of points through which it passes is solved using interpolation techniques. Later, by examining the coefficients of the recovered polynomial, biometric features can be determined. For a polynomial function in degree ν and variable μ, atleast ρ pairs of evaluation points χ_i (may be X/Y/Z) and evaluated value (χ_i, f_i) are required to determine a unique function f using interpolation technique. But the proposed technique generates transformed template Tf blockwise, where $Tf(j)$ is only one point. Here, the claim of non-invertibility of the proposed approach can be established. Since the proposed approach always evaluates the polynomial at only one point, in case of compromise of the user specific token and transformed template, the attacker knows (χ_i, f_i) for only one point. The other $\rho - 1$ sets of evaluation points and its corresponding f_i values are unknown; and hence there are possibilities of infinite solutions. The only means of attack is by using brute force method to find $\rho - 1$ right combinations of (χ_i, f_i) for each feature vector. As there can be infinitely many solutions for a single (χ_i, f_i) combination, this results in a very large key space for brute force to work thus rendering it as practically non-invertible.

VI. Conclusion

The proposed approach is experimentally found to successfully fulfill the important cancelability criteria of revocability, diversity, non-invertibility and performance. Apart from transformation, the proposed approach also reduces dimensionality of the transformed features upto 90%, thereby reducing storage cost and matching time. The performance obtained with the transformed and reduced sized features for all the proposed techniques is as good as ideal and even better than that obtained with original templates in the best-case scenario. Although system performance with reduced transformed features decreases in the worst-case as compared to original features, but not to an extent which becomes unacceptable. Thus a polynomial variant with satisfactory performance in the worst-case can be used to implement a cancelable system.

Acknowledgment

This work is supported by BRNS, DAE, Government of India, Grant. No: 36(3)/14/58/2016-BRNS.

References

[1] "Schneier on security," (Date last accessed 13-March-2017). [Online]. Available: https://www.schneier.com/blog/archives/2015/10/stealing_finger.html

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[3] H. Kaur and P. Khanna, "Biometric template protection using cancelable biometrics and visual cryptography techniques," *Multimedia Tools and Applications*, vol. 75, no. 23, pp. 16 333–16 361, 2016.

[4] N. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: A case study in fingerprints," in *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, vol. 4. IEEE, 2006, pp. 370–373.

[5] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[6] P. Lacharme, E. Cherrier, C. Rosenberger *et al.*, "Preimage attack on biohashing," in *International Conference on Security and Cryptography (SECRYPT)*, 2013.

[7] A. B. Teoh, A. Goh, and D. C. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.

[8] A. B. J. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, no. 5, pp. 1096–1106, 2007.

[9] A. B. J. Teoh, W. K. Yip, and K.-A. Toh, "Cancellable biometrics and user-dependent multi-state discretization in biohash," *Pattern Analysis and Applications*, vol. 13, no. 3, pp. 301–307, 2010.

[10] Y. Wang and K. N. Plataniotis, "An analysis of random projection for changeable and privacy-preserving biometric verification," *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, vol. 40, no. 5, pp. 1280–1293, 2010.

[11] M. Savvides, B. V. Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, vol. 3. IEEE, 2004, pp. 922–925.

[12] E. Maiorana, P. Campisi, and A. Neri, "Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system," in *Systems Conference (SysCon), 2011 IEEE International*. IEEE, 2011, pp. 495–500.

[13] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognition*, vol. 47, no. 3, pp. 1321–1329, 2014.

[14] A. B. J. Teoh and D. C. L. Ngo, "Biophasor: Token supplemented cancellable biometrics," in *Control, Automation, Robotics and Vision, 2006. ICARCV'06. 9th International Conference on*. IEEE, 2006, pp. 1–5.

[15] L. Leng and J. Zhang, "Palmhash code vs. palmphasor code," *Neurocomputing*, vol. 108, pp. 1–12, 2013.

[16] J. Zuo, N. K. Ratha, and J. H. Connell, "Cancelable iris biometric," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*. IEEE, 2008, pp. 1–4.

[17] H. Kaur and P. Khanna, "Cancelable features using log-gabor filters for biometric authentication," *Multimedia Tools and Applications*, pp. 1–22, 2016.

[18] F. Quan, S. Fei, C. Anni, and Z. Feifei, "Cracking cancelable fingerprint template of ratha," in *Computer Science and Computational Technology, 2008. ISCSCT'08. International Symposium on*, vol. 2. IEEE, 2008, pp. 572–575.

[19] F. Farooq, R. M. Bolle, T.-Y. Jea, and N. Ratha, "Anonymous and revocable fingerprint recognition," in *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on*. IEEE, 2007, pp. 1–7.

[20] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *Journal of Network and Computer Applications*, vol. 33, no. 3, pp. 236–246, 2010.

[21] W. Yang, J. Hu, S. Wang, and J. Yang, "Cancelable fingerprint templates with delaunay triangle-based local structures," in *Cyberspace Safety and Security*. Springer, 2013, pp. 81–91.

[22] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognition*, vol. 66, pp. 295–301, 2017.

[23] 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," *Computers & Security*, vol. 65, pp. 373–386, 2017.

[24] 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 Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 393–407, 2018.

[25] S. Cho and A. B. J. Teoh, "Face template protection via random permutation maxout transform," in *Proceedings of the 2017 International Conference on Biometrics Engineering and Application*. ACM, 2017, pp. 21–27.

[26] M. Tamayo-Rios, J.-C. Faugere, L. Perret, P. H. How, and R. Zhang, "Fully homomorphic encryption using multivariate polynomials," *IACR Eprint*, vol. 458, 2017.

[27] S. Cimato and C.-N. Yang, *Visual cryptography and secret image sharing*. CRC press, 2011.

[28] A. B. J. Teoh and J. Kim, "Secure biometric template protection in fuzzy commitment scheme," *IEICE Electronics Express*, vol. 4, no. 23, pp. 724–730, 2007.

[29] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*. IEEE, 2008, pp. 1–4.

[30] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Biometrics Symposium, 2007*. IEEE, 2007, pp. 1–6.

[31] T. Ignatenko and F. M. Willems, "Information leakage in fuzzy commitment schemes," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 337–348, 2010.

[32] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, Sept 2015.

[33] J. Li, N. Sang, and C. Gao, "Log-gabor weber descriptor for face recognition," *Journal of Electronic Imaging*, vol. 24, no. 5, pp. 053 014–053 014, 2015.

[34] M.-H. Yang, "Kernel eigenfaces vs. kernel fisherfaces: Face recognition using kernel methods." in *Fgr*, vol. 2, 2002, p. 215.

[35] G. O. Williams, "The use of d'as a decidability index," in *Security Technology, 1996. 30th Annual 1996 International Carnahan Conference*. IEEE, 1996, pp. 65–71.

[36] CASIA-FaceV5, *Biometrics Ideal Test*, http://biometrics.idealtest.org.

[37] ORL face database, *AT&T Laboratories Cambridge*, http://www.cl.cam.ac.uk/.

[38] S. Z. Li, D. Yi, Z. Lei, and S. Liao, "The casia nir-vis 2.0 face database," in *Computer Vision and Pattern Recognition Workshops (CVPRW), 2013 IEEE Conference on*. IEEE, 2013, pp. 348–353.

[39] IRIS thermal/visible face database, *University of Tennessee*, http://www. cse. ohio-state. edu/otcbvs-bench.

[40] CASIA palmprint database, *Biometrics Ideal Test*, hhttp://biometrics.idealtest.org/downloadDB/.

[41] CASIA-MS-Palmprint V1, *Biometrics Ideal Test*, http://biometrics.idealtest.org.

[42] Y. Yin, L. Liu, and X. Sun, "Sdumla-hmt: a multimodal biometric database," in *Biometric Recognition*. Springer, 2011, pp. 260–268.

[43] M. Gomez-Barrero, J. Galbally, C. Rathgeb, and C. Busch, "General framework to evaluate unlinkability in biometric template protection systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1406–1420, 2018.

[44] C. De Boor and A. Ron, "On multivariate polynomial interpolation," *Constructive Approximation*, vol. 6, no. 3, pp. 287–302, 1990.