Pattern Recognition Letters 000 (2018) 1–10

Contents lists available at ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

Random Slope method for generation of cancelable biometric features

Harkeerat Kaur, Pritee Khanna*

PDPM Indian Institute of Information Technology, Design and Manufacturing, Dumna Airport Road, Jabalpur 482005, India

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Biometrics
Cancelable
Revocable
Random Slope
Stolen token scenario

ABSTRACT

Cancelable biometric templates are transformed versions of original biometric templates used for authentication purposes. The transformation functions should fulfill the important template protection criteria of diversity, revocability, non-invertibility, and performance. Although there exists a number of transformation techniques, yet many of these techniques fail to meet security and privacy requirements in the stolen token scenario and tend to become invertible with degraded performance. The work proposes a novel cancelable biometric technique named as 'Random Slope' method for generating secure, revocable, and non-invertible templates. Two approaches (RS-V1 and RS-V2) developed using the proposed concept not only fulfill the important cancelability criteria, but also provide dimensionality reduction upto 75%. The performances of the proposed approaches are experimentally verified for various biometric modalities such as visible and thermal face, palmprint, palmvein, and fingervein. As compared to some state of the art template transformation schemes, the proposed RS-V1 and RS-V2 approaches establish their reliability and effectiveness by performing better than these existing techniques with significant reduction in dimensions.

1. Introduction

Biometric authentication technology has witnessed a phenomenal growth as the need for accurate and secure authentication has become an absolute necessity. The spectrum of this technology ranges from common applications like mobile phone and laptops to high security applications like military, banking, passports etc. While the use biometric authentication is easy, convenient, and reliable, the tremendous use of this technology has put to risk its own core, '*biometrics*'. Digital biometric identities are most vulnerable to hacking and other malicious activities. Loss of biometric identity at some common and less secure application may proliferate to damage the security of the same biometric used at some security critical application. With cyber crimes growing at alarming rate, the *security of biometric information* has become important for defining *secure access using biometric information* [21]. Apart from security, there are other privacy concerns regarding the use of biometrics. In biometrics, privacy refers to information privacy, i.e., an individual's personal control over the collection, use, and disclosure of recorded information about them, as well as an organization's responsibility for data protection and safeguarding of personally identifiable information in its custody or control [30]. Covert surveillance, sharing of biometric databases without users' consent and cross-matching them are forms of privacy intrusion attacks. Apart from this, biometrics also carries a lot of sensitive and personal information such as gender, ethnicity, and medical conditions. Overall, the loss of biometric identity threatens our security, invokes social and financial losses, invades people's privacy, and thereby produces negative emotional impact on victims.

Various template protection schemes are proposed to bridge the growing gap between '*biometrics for security*' and '*security for biometrics*'. Cancelable biometrics suggests the use of pseudo-biometric identities in place of the original biometric identities [21]. The pseudo-biometric identities are transformed version of original identities generated by using a secure and discriminability preserving transformation function and key. Thus in case of attacks only pseudo-identities are compromised. Also, a biometric information can be mapped to numerous pseudo-identities for usage across different applications by changing the transformation function and/or key, thereby preventing cross-matching and other attacks [20]. This way cancelable biometrics provides high level privacy, security, and revocability to biometrics that may help to increase public confidence for acceptance of biometric based systems.

Designing a technique which fulfills all the important criteria of security, diversity, revocability, and performance is a challenging task. This work proposes a novel concept for biometric transformation named as 'Random Slope' method. The method maps biometric features and some random user-specific data as points on

* Corresponding author.
E-mail address: pkhanna@iiitdmj.ac.in (P. Khanna).

https://doi.org/10.1016/j.patrec.2018.02.016
0167-8655/

Table 1
Some cancelable biometric based template transformation techniques defined in literature.

Category	Technique	Modality
Random Projection	BioHashing [24]	fingerprint
	Random Mutlispace Quantization (RMQ) [23]	face
	Multi-space Random Projections (MRP) [27]	face
	User-dependent Multi-state Discretization (Ud-MsD) [26]	fingerprint
	Sectored random projections [18]	iris
	Random projections with vector translation (RPv) [31]	face
	Dynamic random projections [33]	fingerprint
Random Convolution	Random kernels convolution [22]	face
	BioConvolving [17]	signature
	Curtailed circular convolution [29]	fingerprint
Random Mapping	Cartesian, polar, and surface folding transform [20]	fingerprint
	Cancelable bit strings [9,14]	fingerprint
	Block remapping and image warping [28]	iris
	Random look-up table mapping [8]	iris
	Random Permutation Maxout (RPM) transform [6]	face
Random Noise	BioPhasoring [15,25]	fingerprint, palmprint
	GRAY and BIN salting [37]	iris
	XOR-based salting [12]	visible and thermal face, palmprint, palmvein, fingervein

the Cartesian space. The slopes and intercepts of the lines passing through these features and random points are calculated to generate transformed features. Two approaches proposed on this concept not only generate pseudo-identities, but also provide significant dimension reduction. Matching experiments are performed on various modalities to observe efficacy of the proposed approaches.

The work is organized as follows. Section 2 provides insight to the existing transformation techniques and outlines motivation for the proposed work. Section 3 discusses the Random Slope concept and the proposed template protection approaches are developed in Section 4. Section 5 addresses some relevant issues. The performance of these techniques are analyzed in Section 6. Finally, the work is concluded in Section 7.

2. Literature review

Cancelable biometrics is a transformation based template protection scheme where storage and matching is performed in transformed domain [21]. The two main cancelable approaches used to transform biometrics can be classified as *biometric salting* and *non-invertible transforms* [11]. *Biometric salting* blends independent input factor and user-specific secret key (such as random numbers or passwords) with the biometric data to produces distorted templates. *Non-invertible transform* uses some user-specific secret key as parameter for the transformation function to generated transformed biometric templates. The secret key is generated externally and interacts with the biometric template to increase its entropy using any of the above transformation techniques. In case of a compromise, it is easy to revoke and generate a new template by changing the key. Considering their ability to satisfy desirable properties, i.e., *non-invertibility, discriminability*, and *revocability*, the major techniques under which these approaches can be classified are summarized in Table 1 and discussed below.

Random Projection based Transformations: Random projection (RP) forms basis of the most biometric salting techniques that exist in literature. Based on Johnson and Lindenstrauss lemma, the technique essentially involves projection of biometric data over a random sub-space to generate salted biometric features. The method preserves discriminability by preserving the pair-wise distances of feature points before and after projection. BioHashing is the most popular biometric salting technique [24]. The biometric features are salted by projecting them on orthonormal random subspace. Projected features are quantized into binary codes via thresholding operations to achieve a many-to-one mapping and thus ensure non-invertibility. BioHashing essentially uses orthonormal random matrices for projection purposes which involve high computational process like Gram-Schmidt orthonormalization. Although the approach preserves discriminability, it is susceptible to inverse operations if the transformed biometric and projection matrix are simultaneously known to the attacker [13]. Various techniques such as Random Mutlispace Quantization (RMQ) in BioHash [23], Multi-space Random Projections (MRP) [27], User-dependent Multi-state Discretization (Ud-MsD) BioHash [26], Sectored Random Projections [18], Random Projection with vector translation [31], and Dynamic Random Projections [33] are proposed to improve upon the drawbacks.

Random Convolution based Transformations: Initially, a simple convolution method using Minimum Average Correlation Energy (MACE) filters was proposed for generating face biometric features [22]. If random kernel used during convolution is known, then deconvolution can be attempted to recover features. A novel technique known as BioConvolving uses some random user-specific key to divide the original features into fixed sized segments that are later convolved according to the user-specific data for generating transformed templates [17]. However, the discriminability preserving property is not justified for stolen token scenario when the same keys are used for each subject. Further, if convolution kernel and key are simultaneously known, then de-convolution attempts may tend to compromise the invertibility of the approach. Curtailed circular convolution is proposed to generate non-invertible cancelable fingerprints with good matching performance [29]. The proposed algorithm requires the input features to be in a binary format which are later convolved with random binary strings in circular manner. The convolved results are curtailed to impart non-invertibility.

Random Mapping or Permutation based Transformations: Cartesian, polar, and surface folding transform are three random mapping functions which are used to distort fingerprint minutiae points to a new subspace in a many-to-one fashion [20]. Although the authors claimed that the transforms are non-invertible, approximation of the original data is possible when the transformed templates and parameters are simultaneously available to the attacker [19]. Cancelable bit strings from minutiae features are also proposed [9,14]. The technique randomly maps minutiae features onto a predefined 3D array based on some user-specific key and reference minutia's position and orientation. The technique involves many to one mapping of minutia points to bit string which may affect the overall discriminability of transformed features. Also, the non-invertibility can be compromised when the bit string

Please cite this article as: H. Kaur, P. Khanna, Random Slope method for generation of cancelable biometric features, Pattern Recognition Letters (2018), https://doi.org/10.1016/j.patrec.2018.02.016

and user-specific key are known to the attacker. Block remapping and image warping procedures are utilized to generate cancelable iris templates [28]. Normalized iris image is divided into random blocks and subjected to random permutation. Although the scheme does not compromise on accuracy, but it is found that as much as 60% of the original template can be restored if the stolen template and permutation key are available [10]. A technique for cancelable iris templates is proposed by using randomized look-up table mapping [8]. The method extracts consistent bits from feature vectors to generate a decimal value which is randomly mapped using a look-up table. However, if the look-up table and transformation parameters are known, the mapping can be inverted. Another permutation technique known as random permutation maxout transform maps a real-valued face feature vector into a discrete index code that can be used as a transformed template [6].

Random Noise based Transformations: This set of techniques distorts biometric templates by adding some random noise patterns. BioPhasoring, GRAY salting, and XOR-based salting are three major techniques under this category. BioPhasoring generates a set of complex vectors where the original features form the real part and the user-specific random vectors form the imaginary part [25]. The phase/arctangent of the complex vector is computed, which is non-invertible, and is used as transformed template. BioHashing and BioPhasoring techniques are also improvised for palmprint modality [15]. The authors extended transformation algorithm from 1D to 2D for both the techniques to generate transformed templates with reduced computational complexity and storage cost. They also indicated that the above coding schemes can be extended to other modalities like fingervein, palmvein etc. GRAY salting (template based salty noise) adds random noise patterns or a synthetic texture to a biometric template at image level to generate a new transformed template. GRAY salting is implemented with Gabor features extracted from transformed templates obtained for iris biometrics [37]. Another variant of this technique, known as BIN salting (code based salty noise), extracts binary features from the input image which is salted using binary patterns [37]. Both GRAY and BIN salting are subjective to inverse attacks if the salting parameter is known. In another noise based salting approach, transformed templates are generated by XORing original features with random patterns followed by non-linear median filtering operations such that non-invertibility and discriminability is preserved for the salted template [12].

The following shortcomings are observed from the literature:

1. Most of the transformation techniques are susceptible to inverse operations in case the transformed template and user specific key are simultaneously known to the attacker (stolen token scenario).
2. The performance is determined only in the best-case scenario for many techniques, which assumes that the user-specific key is never compromised. The performance must also be determined for the worst-case scenario when the secret key is assumed to be known to the attacker.
3. Applicability of most techniques is verified for a specific modality and usually its performance other modalities is not reported or defined. For e.g., applicability of most mapping techniques is limited to fingerprint modality.

This work proposes a novel biometric transformation scheme called *Random Slope method* that address the above issues. The approaches aims to generate secure, revocable, non-invertible, privacy preserving, and performance preserving templates even in stolen token scenario.

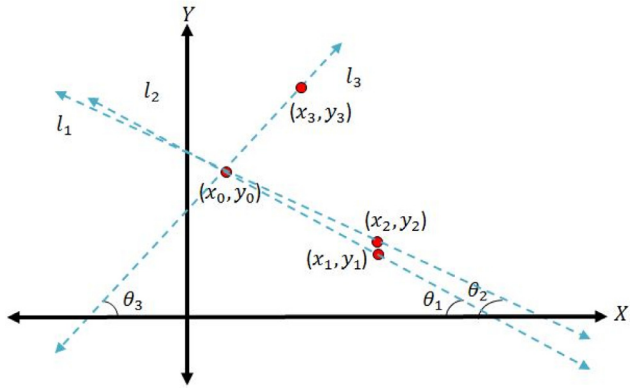

Fig. 1. The concept of Random Slope method.

3. The Random Slope concept

Let a feature vector fv be represented as a point in Cartesian subspace. Then, instead of using the original **biometric** feature vector fv, slope and intercepts of the line joining this feature point with some random point can be used for matching purposes. The concept is illustrated in Fig. 1.

Let the feature vector be divided into two equal halves such that the j^{th} value in each half is used to define a point in Cartesian space as $(x, y) \in fv$. Let (x_1, y_1), (x_1, y_2), and (x_3, y_3) be point representations of feature vectors fv_1, fv_2, and fv_3; and (x_0, y_0) is a random point derived from user-specific key. Assume that the same key is assigned to each user (worst-case scenario). Then l_1, l_2, and l_3 are lines passing through these feature vector points and random point. The general equation of line in slope-intercept form is $y = \mathtt{m}x + \mathtt{c}$, where $\mathtt{m}$ stands for slope or gradient and $\mathtt{c}$ is the intercept made by the line. The idea is to use the slopes $\mathtt{m}_1$, $\mathtt{m}_2$, and $\mathtt{m}_3$ and intercepts $\mathtt{c}_1$, $\mathtt{c}_2$, and $\mathtt{c}_3$ of lines l_1, l_2, and l_3 in place of the original feature values (x_1, y_1), (x_1, y_2), and (x_3, y_3). The slopes and intercepts of line l_1 passing through (x_1, y_1) and (x_0, y_0), line l_2 through (x_1, y_2) and (x_0, y_0), and line l_3 through (x_1, y_3) and (x_0, y_0) are calculated as

$$\mathtt{m}_1 = \frac{y_1 - y_0}{x_1 - x_0}, \mathtt{m}_2 = \frac{y_2 - y_0}{x_1 - x_0}, \mathtt{m}_3 = \frac{y_3 - y_0}{x_1 - x_0} \text{ and}$$

$$\mathtt{c}_1 = (y_0 - y_1) - \mathtt{m}_1 x_1, \mathtt{c}_2 = (y_0 - y_2) - \mathtt{m}_2 x_2, \mathtt{c}_3 = (y_0 - y_3) - \mathtt{m}_3 x_3$$

If the feature vectors fv_1 and fv_2 belong to the same user, then the difference in their values will be small, i.e., $x_1 - x_2 < \delta$ and $y_1 - y_2 < \delta$. It can be shown that the difference in the slope and intercepts, i.e., $\mathtt{m}_1 - \mathtt{m}_2 < \delta$ and $\mathtt{c}_1 - \mathtt{c}_2 < \delta$ will also be small in order to preserve intra-user variations.

To Prove : $\mathtt{m}_1 - \mathtt{m}_2 < \delta$

Proof.

$$\text{Let } ||x_1 - x_2|| = \delta \text{ and } ||y_1 - y_2|| = \delta$$

$$\text{Now, } \mathtt{m}_1 - \mathtt{m}_2 = \frac{y_1 - y_0}{x_1 - x_0} - \frac{y_2 - y_0}{x_2 - x_0}$$

$$= \frac{y_2 + \delta - y_0}{x_2 + \delta - x_0} - \frac{y_2 - y_0}{x_2 - x_0}$$

$$= \frac{(y_2 - y_0) + \delta}{(x_2 - x_0) + \delta} - \frac{y_2 - y_0}{x_2 - x_0}$$

$$\text{Let, } a = (y_2 - y_0) \text{ and } b = (x_2 - x_0)$$

$$\mathtt{m}_1 - \mathtt{m}_2 = \frac{a + \delta}{b + \delta} - \frac{a}{b}$$

$$= \frac{a}{b + \delta} - \frac{a}{b} + \frac{\delta}{b + \delta}$$

$$= \frac{ab - ab - a\delta}{b(b+\delta)} + \frac{\delta}{b+\delta}$$
$$= \frac{\delta}{b+\delta} - \frac{a}{b}\frac{\delta}{b+\delta}$$
$$\text{let } \delta' = \frac{\delta}{b+\delta} \text{ , then } \delta' < \delta$$
$$= \delta' - \frac{a}{b}\delta' < \delta$$
$$\text{Thus, } \quad \mathtt{m}_1 - \mathtt{m}_2 < \delta \ \textbf{\textit{Hence Proved.}}$$

□

To Prove : $\mathtt{c}_1 - \mathtt{c}_2 < \delta$

Proof.

Again, $||x_1 - x_2|| = \delta$ and $||y_1 - y_2|| = \delta$

$$\text{Now, } \mathtt{c}_1 - \mathtt{c}_2 = ((y_0 - y_1) - \mathtt{m}_1 x_1) - ((y_0 - y_2) - \mathtt{m}_2 x_2)$$
$$= (y_2 - y_1) + (\mathtt{m}_2 x_2 - \mathtt{m}_1 x_1)$$
$$= \delta + (\mathtt{m}_2 x_2 - \mathtt{m}_1 (x_2 + \delta))$$
$$= \delta - x_2(\mathtt{m}_1 - \mathtt{m}_2) - \mathtt{m}_1 \delta$$
$$\text{Thus, } \quad \mathtt{c}_1 - \mathtt{c}_2 < \delta \ \textbf{\textit{Hence Proved.}}$$

□

Thus $(fv_2 - fv_1) \propto (\mathtt{m}_2 - \mathtt{m}_1) \propto (\mathtt{c}_2 - \mathtt{c}_1) \propto \delta$. On the same line, if the feature vectors fv_1 and fv_3 belong to different users, then the difference between their values would be large, i.e., $(fv_3 - fv_1) \propto \Delta$ and $(\mathtt{m}_3 - \mathtt{m}_1) \propto (\mathtt{c}_3 - \mathtt{c}_1) \propto \Delta$. Thus, inter and intra-user variations are maintained using the random slope concept.

4. Proposed feature transformation approaches

Two feature transformation techniques are developed on the basis of random slope concept. Before applying the transformation, the input signal image is preprocessed for removal of noise, extraction of ROI, followed by feature extraction. The extracted features are subjected to transformation.

Preprocessing: The proposed approach uses log-Gabor filters for efficient feature extraction of a preprocessed biometric image signal at various frequency resolutions. The log-Gabor filters are an improvement to Gabor filters and are used here to resolve the image signal at $n = 4$ scales and $m = 6$ orientations. The details of feature extraction using log-Gabor filters can be found in [12]. Let I be a preprocessed biometric signal image of dimensions $M \times N$, here $M = N = 128$. The output of filter response is a complex value from which magnitude patterns are computed. For each scale and orientation the obtained patterns are added, 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 $N' = 24 \times 128 \times 128$ is the total number of features.

Proposed Approach-1 **(RS-V1)**: Initially, the original feature vector fv is salted using RG and OR operation.

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

A user-specific random grid RG with dimension same as that of fv is generated, which possesses random integral values in the desired range, e.g., [-255 to 255]. The salted vector fs is divided into two equal parts $fX = fs(1 : N'/2)$ and $fY = fs(N'/2 + 1 : N')$. The feature point FP_j is defined using the values corresponding to the two vectors $(x_j = fX(j), y_j = fY(j))$ for $j = 1...N'/2$. A user-specific key $\mathcal{K}$ of dimension $1 \times N'$ is generated having 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 equation of line l_j passing through feature point FP_j and random point RP_j is established and the slope $\mathtt{m}_j$ and intercept $\mathtt{c}_j$ of all such lines are recorded as vector $\mathtt{M} = \{\mathtt{m}_j\}$ and $\mathtt{C} = \{\mathtt{c}_j\}$. Vector $\mathtt{M}$ and $\mathtt{C}$ are normalized as

$$\mathtt{M}'_j = \frac{\mathtt{M}_j - min(\mathtt{M})}{max(\mathtt{M}) - min(\mathtt{M})}, \mathtt{C}'_j = \frac{\mathtt{C}_j - min(\mathtt{C})}{max(\mathtt{C}) - min(\mathtt{C})} \tag{2}$$

The normalized slope and intercept vectors are added to form the transformed template $Tf(j) = \mathtt{M}'(j) + \mathtt{C}'(j)$. Instead of the original feature fv, the transformed feature Tf is used for storing and matching purposes. The vectors RG and $\mathcal{K}$ are provided to the user in a tokenized format. At every authentication, users' biometric is transformed using the same vectors. If compromised, new transformed template can be generated by changing the keys. Also, the dimension of transformed features reduces by 50%. The concept is illustrated in Fig. 2(a).

Proposed Approach-2 **(RS-V2)**: Another variant is proposed which allows feature dimension to be reduced by a factor of 1/4. The concept is illustrated in Fig. 2(b). This variant divides the salted vector fs into four equal parts, fX_1, fY_1, fX_2, and fY_2, each of dimension $1 \times N/4$. The user specific key $\mathcal{K}$ of dimension $1 \times N/2$ is randomly generated and divided into two equal parts $\mathcal{K}_0$ and $\mathcal{K}_1$ as above. The salted feature vector can now be mapped as two points $FP_{1j}(x_j = fX_1(j), y_j = fY_1(j))$ and $FP_{2j}(x_j = fX_2(j), y_j = fY_2(j))$, and key $\mathcal{K}$ as a random point $RP_j(x_j = \mathcal{K}_0(j), y_j = \mathcal{K}_1(j))$ for $j = 1...N/4$. A line is established between each feature point and random point and the angle between the two lines can be used as the transformed value. The line l_{1j} between point FP_{1j} and RP_j has slope $\mathtt{m}_{1j}$ and line l_{2j} between point FP_{2j} and RP_j has slope $\mathtt{m}_{2j}$. The angle α between these two lines l_{1j} and l_{2j} is computed as

$$\alpha = \frac{\mathtt{m}_{1j}.\mathtt{m}_{2j}}{1 + \mathtt{m}_{1j}.\mathtt{m}_{2j}} \tag{3}$$

The transformed vector Tf is concatenation of angle between lines passing through each pair of points, $Tf(j) = \alpha_j$ for $j = 1...N/4$. This vector is also revocable by changing user-keys and allows dimensionality reduction by three-fourth, i.e., 75%.

5. Some illustrative examples and relevant issues

Point-Set Distribution in the Original and Transformed Domain: The intra and inter-user point-set distributions of original, salted, and transformed features for samples belonging to CASIA-NIR face database are illustrated in Figs. 3 and 4 respectively. For each biometric sample image, features are extracted using log-Gabor transform. The first 100 values obtained at $n = 1$ scale and $m = 1$ orientation are used for plotting purposes. Fig. 3(a) and (b) show sample images I_1 and I_2 belonging to the same subject. Mapping of their original features is shown in Fig. 3(c). The RS-V1 approach divides the salted feature into two halves to map x, y-coordinates of feature points. Fig. 3(d) depicts the feature points obtained from salted features and the random points obtained from key $\mathcal{K}$. The transformed features for RS-V1 obtained from the two samples and key $\mathcal{K}$ are plotted in Fig. 3(e). Further, Fig. 3(f) depict the two sets (A and B) into which the salted feature points are divided as defined in approach RS-V2. Lines are defined using features points belonging to these two sets and random points. The angle between these lines is calculated as transformed features, which are plotted in Fig. 3(g). The mapping of features points shown in the figures illustrate the distortion of original features, increase in entropy, and preservation of intra and inter-user variations of biometric features in the transformed domain.

Some Ambiguous Cases: The proposed approaches makes use of slope and intercept of lines and angle between two lines to generate revocable features. Again there are chances that these values tend to become the same for features belonging to different users. The ambiguous condition for RS-V1 is when j^{th} feature points of

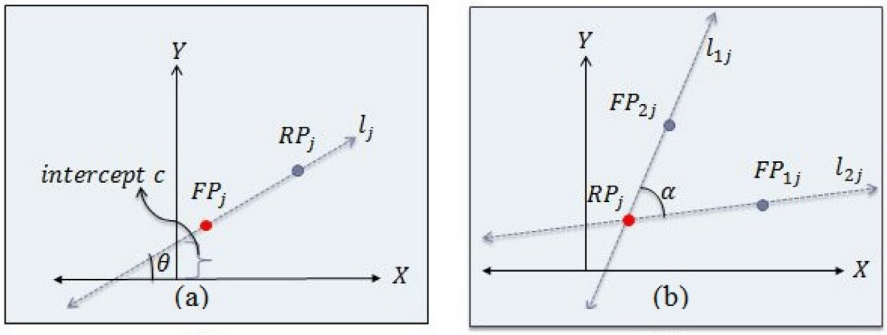

Fig. 2. Concept illustrations (a) Proposed approach-1 (RS-V1) and (b) Proposed approach-2 (RS-V2).

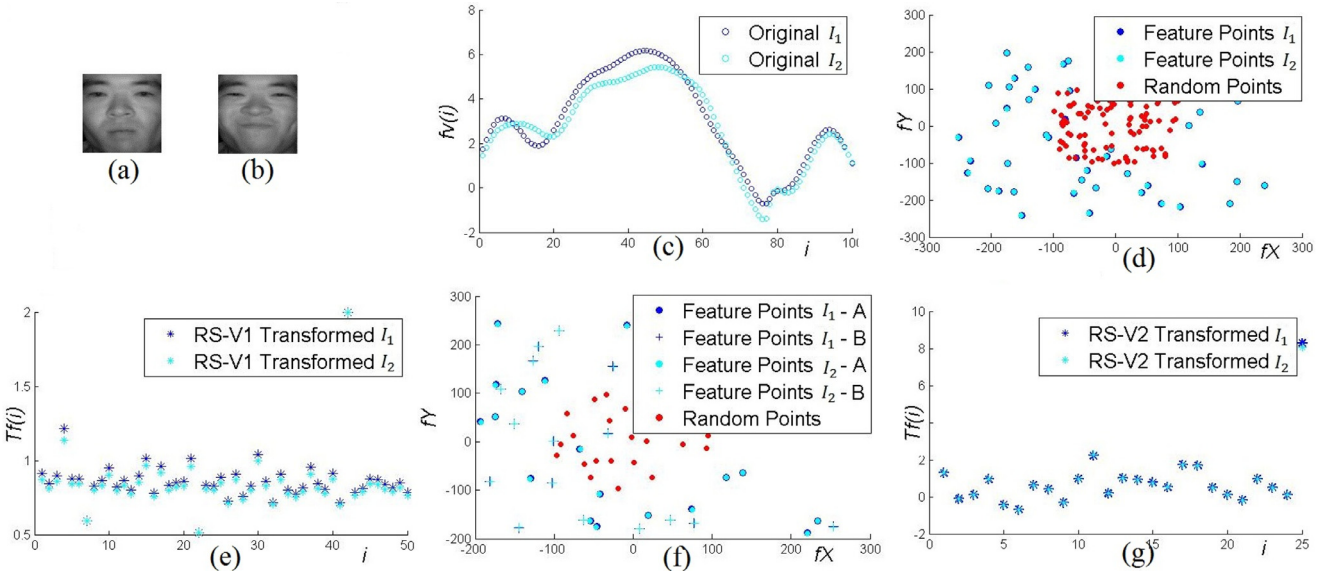

Fig. 3. Point-set distributions illustrating intra-user variations for CASIA-NIR face (a)-(b) sample images I_1 and I_2, (c) original features, (d) feature points and random points for RS-V1, (e) transformed features RS-V1, (f) feature points (set A, B) and random points for RS-V2, and (g) transformed features RS-V2.

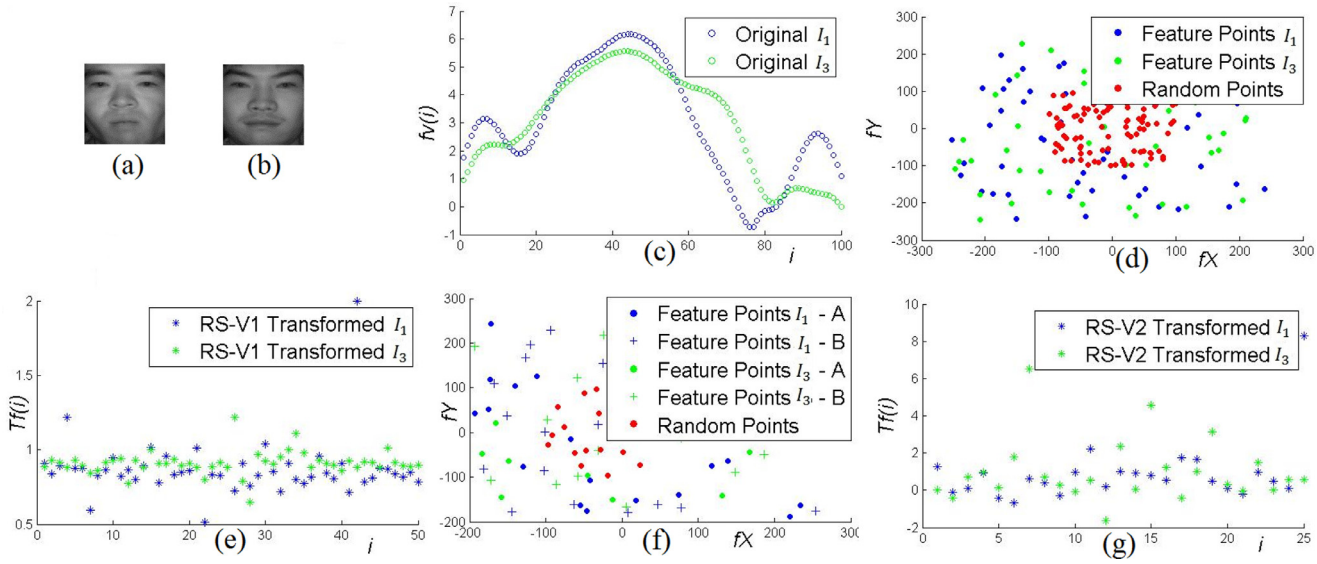

Fig. 4. Point-set distributions illustrating inter-user variations for CASIA-NIR face (a)-(b) sample images I_1 and I_3, (c) original features, (d) feature points and random points for RS-V1, (e) transformed features RS-V1, (f) feature points (set A, B) and random points for RS-V2, and (g) transformed features RS-V2.

Please cite this article as: H. Kaur, P. Khanna, Random Slope method for generation of cancelable biometric features, Pattern Recognition Letters (2018), https://doi.org/10.1016/j.patrec.2018.02.016

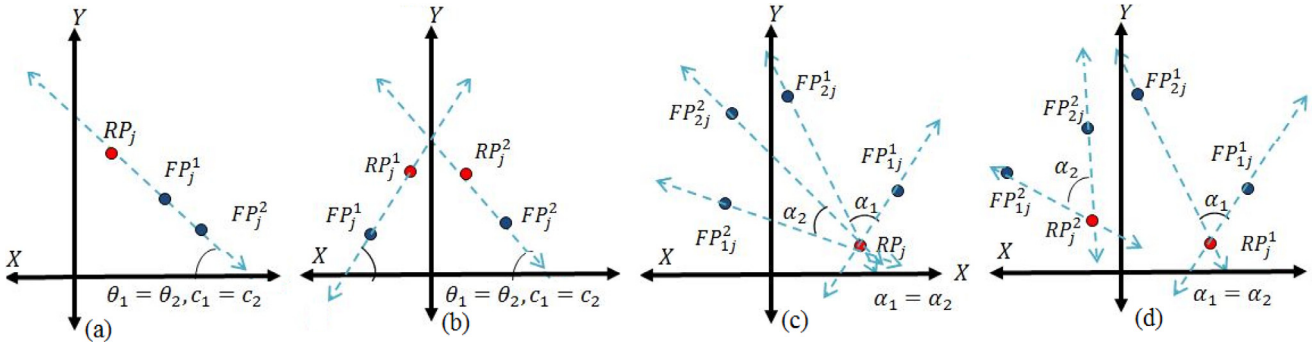

Fig. 5. Some ambiguous cases (a) RS-V1: worst-case scenario, (b) RS-V1: best-case scenario, (c) RS-V2: worst-case scenario, and (d) RS-V2: best-case scenario.

Table 2
Databases used for experimentation.

Modality	Database	Subjects	Samples /subject	k- fold
Face	CASIA-Face V5 [4]	500	5	5
	ORL [1]	40	10	5
Thermal	CASIA NIR [16]	197	10	5
Face	IRIS [7]	29	10	5
Palmprint	CASIA Palmprint [2]	301	8	4
	PolyU [36]	386	10	5
Palmvein	CASIA-MS V1 [3]	200	6	6
Fingervein	SDUMLA-HMT [35]	636	6	6

two different users (FP_j^1 and FP_j^2) tend to make same slope and intercept with the same random point (RP_j) in the worst-case scenario and with different random points (RP_j^1 and RP_j^2) in the best-case scenario, respectively as illustrated in Fig. 5(a) and (b). Similarly for the second variant RS-V2, the ambiguous conditions arising in the worst and best-case scenario are illustrated in Fig. 5(c) and (d). For the transformed templates arising from two different features to be same, such situations must come true for more than 60% to –75% of points in the worst or best-case scenario. The image sample used here for experimentation is of dimension 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. As the feature size is quite large, the possibility of transformed features becoming same for more than 60% to 75% of features size is less. To determine the possibility of such conditions in the worst and best-case scenarios, a number of transformed templates are generated by changing key $\mathcal{K}$ and experimentally verified for matching and changeability performance in the next section.

6. Experimental results and discussions

This section reports the results when matching is performed on transformed templates belonging to several standard databases of different visible and thermal biometrics modalities. Table 2 provides details of the databases used for face, thermal face, palmprint, palmvein, and fingervein modalities along with the number of subjects per database. The approach is experimentally analyzed and discusses for various properties like matching performance, changeability, and non-invertibility.

6.1. Performance analysis

As matching is performed in the transformed domain, transformed templates consisting of random slopes and intercepts must preserve the essence of biometric information and their matching performance should not decrease as compared to the original templates. Transformed templates are generated for worst-case and best-case scenario to find the discriminability of the proposed approaches.

***Evaluation Methods*:** All templates used for experimentation are resized to 128×128 pixels. 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 2. Later, classification and matching is performed using Kernel Discriminant Analysis (KDA) and cosine distances [34]. KDA uses a kernel function, which defines a non-linear mapping for feature vectors that exhibit significant variations such that features can be linearly separable and the most significant discriminating information can be easily extracted.

Fasle Accept Rate (*FAR*) and False Reject Rate (*FRR*) are important and basic performance measures of the matching process. They are closely related and defined by the system threshold function value τ. In practice, the most challenging aspect is to obtain a zero score for *FAR* and *FRR*. The impact of rejection in a biometric system must be as low as possible. Therefore, another index of performance has been used in the form of a point where *FAR* and *FRR* will be equal. This point is known as the *Equal Error Rate* (*EER*). The lower the *EER*, the better the system performance. For an ideal biometric system the *EER* score is zero. Another useful parameter is *Decidability Index* (*DI*), which measures the separability of genuine and imposter classes. *DI* is defined as the normalized distance between means of genuine (μ_g) and imposter (μ_i) distributions [32]. It measures the confidence in classifying patterns for a given classifier. Higher values of *DI* indicate better decidability while classifying genuine and imposter populations. *DI* is calculated as

$$DI = \frac{|\mu_g - \mu_i|}{\sqrt{(\sigma_g^2 + \sigma_i^2)/2}} \tag{4}$$

Hence, for verification mode the performance is reported in terms of *EER* and *DI*, which are supported by Receiver Operating Characteristic (ROC) curves.

***Comparison Techniques*:** Matching experiments are also performed for six state of the art techniques belonging to different feature transformation categories namely, Gray Salting [37], Random Projection with vector translation [31], BioConvolving [17], 2D BioPhasor with adaptive thresholding [15], XOR based salting [12], and Random Permutation Maxout (RPM) transform [6]. Random Projection with vector translation (RPv) is implemented for its three variants namely - RPv, RPv-50, and RPv-75, where dimensionality of the transformed features is reduced to 50% in RPv-50 and 75% in RPv-75 by means of random projection. Two variants of XOR based salting are proposed in [12]. For the first variant (XOR), the original features are xored with random patterns followed by non-linear median filtering and desampling to generate transformed templates with 50% reduced dimensionality. In the

Table 3
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	PolyU	CASIA-MS V1	SDUMLA-HMT
-	Original	2.17 ± 0.99	0.85 ± 0.23	1.83 ± 0.41	0.19 ± 0.08	0.33 ± 0.11	0.42 ± 0.15	0.63 ± 0.21	0.47 ± 0.21
	Gray Salting	4.71 ± 1.59	1.27 ± 0.61	5.36 ± 1.25	2.42 ± 0.82	0.65 ± 0.31	1.02 ± 0.83	2.19 ± 0.46	1.04 ± 0.64
	RPv	2.92 ± 1.26	1.16 ± 0.67	2.63 ± 0.37	0.38 ± 0.12	0.53 ± 0.17	0.60 ± 0.23	0.81 ± 0.34	0.71 ± 0.32
	BioPhasor	3.60 ± 1.29	2.59 ± 0.51	5.67 ± 1.32	1.39 ± 0.46	1.36 ± 0.51	1.30 ± 0.33	2.01 ± 0.87	1.49 ± 0.58
	BioConvolving	7.84 ± 1.07	2.50 ± 0.46	3.80 ± 0.89	7.20 ± 1.15	2.88 ± 0.87	5.95 ± 1.32	5.50 ± 0.95	2.20 ± 0.62
	RPM	9.28 ± 3.08	6.75 ± 2.42	7.30 ± 4.86	13.49 ± 5.07	4.00 ± 1.37	2.91 ± 1.50	4.50 ± 2.38	1.73 ± 0.62
50%	Proposed RS-V1	2.40 ± 1.12	0.99 ± 0.46	2.21 ± 0.59	0.22 ± 0.10	0.42 ± 0.15	0.48 ± 0.17	0.68 ± 0.24	0.51 ± 0.32
	XOR	2.78 ± 1.03	1.33 ± 0.86	2.64 ± 0.78	0.41 ± 0.13	0.55 ± 0.22	0.60 ± 0.22	1.03 ± 0.35	0.66 ± 0.24
	RPv-50	3.35 ± 0.90	1.63 ± 0.46	3.57 ± 1.23	0.54 ± 0.23	0.68 ± 0.31	0.67 ± 0.19	1.50 ± 0.63	0.78 ± 0.32
75%	Proposed RS-V2	3.08 ± 2.11	1.19 ± 0.19	2.80 ± 0.82	0.36 ± 0.12	0.52 ± 0.29	0.64 ± 0.35	1.11 ± 1.01	0.68 ± 0.26
	RP-XOR	3.65 ± 1.35	1.87 ± 0.78	3.51 ± 1.24	0.52 ± 0.15	0.72 ± 0.31	0.91 ± 0.33	1.22 ± 0.41	0.90 ± 0.27
	RPv-75	3.92 ± 1.16	2.50 ± 0.76	4.66 ± 1.26	1.03 ± 0.25	0.88 ± 0.36	0.71 ± 0.26	2.17 ± 0.59	2.50 ± 0.97

Table 4
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	PolyU	CASIA-MS V1	SDUMLA-HMT
-	Original	4.588 ± 1.390	5.526 ± 1.232	4.712 ± 1.121	5.773 ± 1.746	8.521 ± 1.960	8.399 ± 1.330	6.469 ± 1.512	5.790 ± 1.424
	Gray Salting	3.596 ± 0.428	5.112 ± 0.124	4.105 ± 0.138	4.310 ± 0.188	7.896 ± 1.154	7.914 ± 0.125	4.850 ± 0.218	3.921 ± 0.420
	RPv	4.412 ± 1.011	5.309 ± 0.332	4.328 ± 0.472	5.454 ± 0.306	7.151 ± 1.760	8.120 ± 0.325	5.979 ± 0.214	4.314 ± 0.385
	BioPhasor	3.112 ± 1.021	4.149 ± 0.021	4.025 ± 0.121	3.857 ± 0.305	6.692 ± 1.157	5.040 ± 0.273	5.036 ± 0.114	4.050 ± 1.130
	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	3.721 ± 0.033
	RPM	2.577 ± 0.385	2.954 ± 0.388	3.617 ± 0.825	2.636 ± 0.424	5.351 ± 1.441	4.065 ± 0.405	3.383 ± 0.60	3.747 ± 0.033
50%	Proposed RS-V1	4.456 ± 1.243	5.282 ± 1.321	4.521 ± 1.592	5.612 ± 1.942	7.523 ± 2.101	8.259 ± 1.321	6.210 ± 1.629	5.498 ± 1.533
	XOR	4.401 ± 1.021	4.432 ± 1.104	4.475 ± 0.987	5.217 ± 1.231	7.214 ± 1.254	8.118 ± 1.254	5.352 ± 1.221	4.921 ± 1.332
	RPv-50	3.454 ± 0.280	4.729 ± 0.332	4.213 ± 0.121	5.183 ± 0.251	7.021 ± 1.121	7.685 ± 0.287	5.141 ± 0.212	4.111 ± 1.054
75%	Proposed RS-V2	4.408 ± 1.321	5.126 ± 1.332	4.510 ± 0.998	5.388 ± 1.433	7.338 ± 1.747	8.110 ± 1.643	5.280 ± 1.345	4.788 ± 1.412
	RP-XOR	3.420 ± 1.311	4.112 ± 1.201	3.987 ± 0.987	5.102 ± 1.121	6.587 ± 1.540	7.985 ± 1.987	4.874 ± 1.334	4.103 ± 1.651
	RPv-75	3.218 ± 0.241	4.415 ± 0.133	4.123 ± 0.113	5.121 ± 0.113	6.814 ± 1.191	6.313 ± 0.437	4.917 ± 0.136	3.978 ± 1.124

second variant (RP-XOR), dimension of the image is reduced by RP followed by XOR; and then median filtering and desampling is performed to generate transformed templates with 75% reduced size. There is no provision of dimensionality reduction for Gray salting, BioPhasor, and BioConvolving. BioConvolving and Random Permutation Maxout transform are implemented according to their best parameter definitions described in [6,17]. The transformed templates generated by using these techniques on log-Gabor features (*fv*) are used to evaluate the proposed approaches, so that the distortion affect can be compared on the same scale.

Evaluation Scenarios: *Worst-case* or *Stolen token scenario* tests the performance of the system assuming that an attacker can always obtain the user-specific tokens. Further, each template is transformed on the same scale to find the extent to which the transform preserves discriminating characteristics. It is therefore expected that the matching performance in transformed domain should be similar to the original domain (untransformed features). To simulate the worst case, each user in the database is assigned the same key variables, i.e., *RG* and *K* in this case.

Similarly for the other comparison techniques, same key varaibles are used accordingly. Tables 3 and 4 report *EER* and *DI* respectively for the proposed approaches RS-V1 and RS-V2 in the worst-case scenario at the significance level of 95%. It is observed that the technique gives comparable results to baseline approach (original features without any transformation) which establishes the fact that the proposed transformation does not sacrifice discriminability.

It is observed that both the proposed approaches RS-V1 and RS-V2 perform better than Gray salting and BioPhasor. Also, the proposed schemes outperform the matching performance of convolution based BioConvolving and permutation based RPM approaches. It is found that the RS-V1 (at 50% reduction) performs better than RPv (at no reduction) and XOR based salting (at 50% reduction). Also, performance of RS-V2 (at 75% reduction) is better than RPv-50 (at 50% reduction) and RP-XOR (at 75% reduction). The above comparisons indicate that the transformed templates generated with the proposed RS-V1 and RS-V2 approaches give better matching performance with significant reduction in dimensions. The ROC curves corresponding to the results reported in Table 3 are shown in Figs. 6 and 7.

Best-case or *legitimate token scenario* assumes the transformation key is always secure and is simulated by assigning different transformation keys *RG* and $\mathcal{K}$ to each user in the database. Different transformation parameters for each user significantly enhance inter-user variations, resulting in very low *EER* values ($< 0.01E-10$) and high *RI* ($> 99.\overline{99}$) values in the best-case scenario. The *DI* values for both the approaches are reported in Table 5. It is observed that *DI* values are significantly high for both the proposed approaches, i.e., $DI(>27)$ for RS-V1 and $DI(>17)$ for RS-V2. This indicates high separability and supports low error rates as a result.

6.2. Changeability analysis

Correlation analysis is performed to determine the revocability and diversity properties of the transform. Generating transformed templates by using different random grid *RG* is straightforward. Changeability is analyzed here to determine the affect of key $\mathcal{K}$. For both the approaches, different transformed templates are generated from each sample in the database by changing key $\mathcal{K}$ and mutual information content C_r is evaluated. The correlation index (*CI*) is the mean of all collected C_r values. A *CI* value equal to 0.105 means 10.5% of mutual information is present between two set of transformed templates. Usually, mutual information content

Please cite this article as: H. Kaur, P. Khanna, Random Slope method for generation of cancelable biometric features, Pattern Recognition Letters (2018), https://doi.org/10.1016/j.patrec.2018.02.016

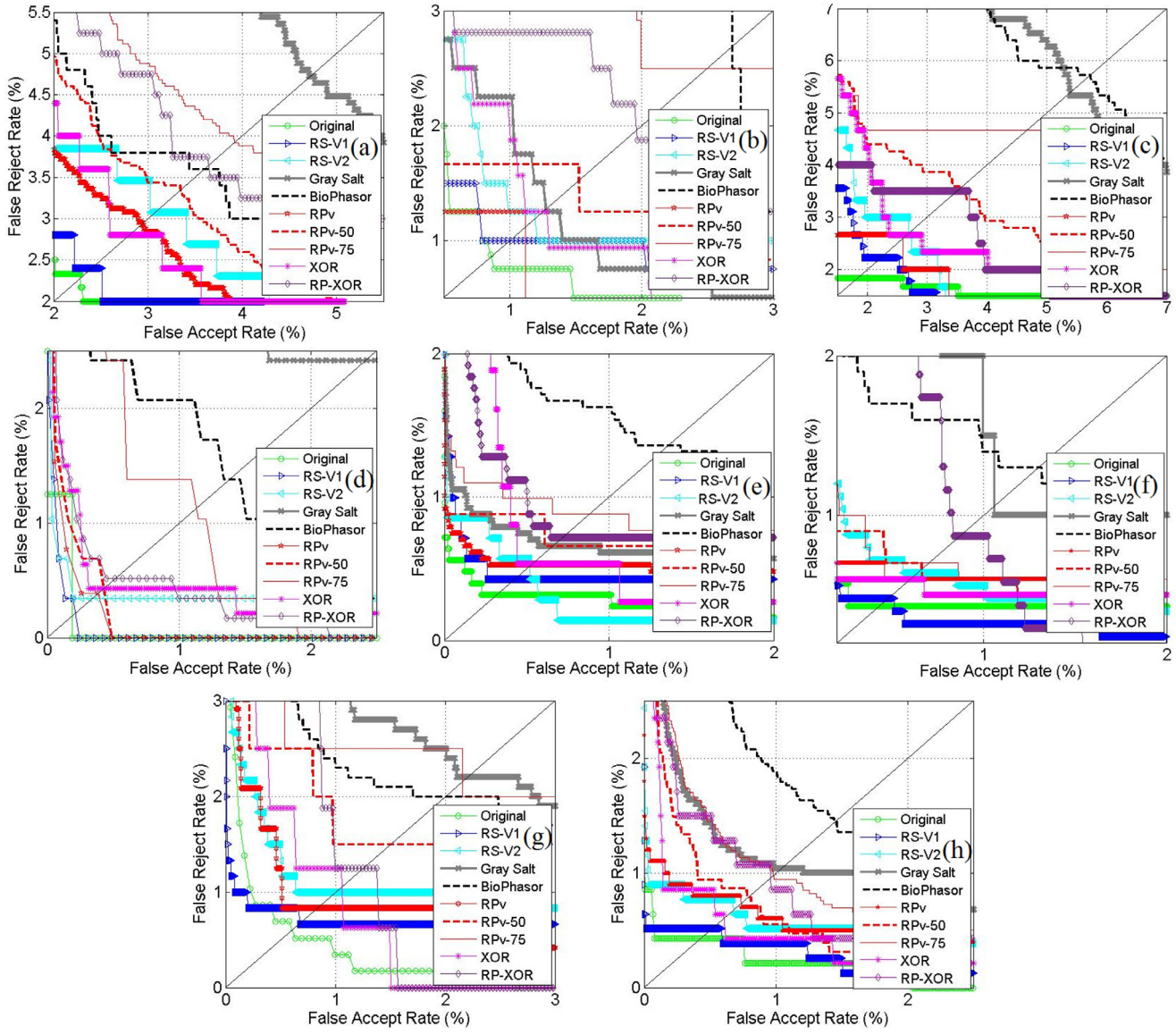

Fig. 6. ROC curves in the worst-case scenario (a) CASIA V5, (b) ORL, (c) CASIA NIR V5, (d) IRIS, (e) CASIA, (f) PolyU, (g) CASIA-MS V1 (940nm), and (h) SDUMLA-HMT.

Table 5
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	PolyU	CASIA-MS V1	SDUMLA-HMT
Proposed RS-V1	30.936 ± 1.515	32.210 ± 1.841	28.308 ± 1.214	27.316 ± 1.521	34.875 ± 1.024	33.983 ± 1.784	27.475 ± 1.321	28.154 ± 1.087
Proposed RS-V2	17.510 ± 1.014	20.124 ± 1.106	18.931 ± 1.112	17.817 ± 1.231	19.036 ± 1.410	18.667 ± 1.251	17.060 ± 1.511	18.514 ± 1.201

Table 6
Correlation index (*CI*%) values for the proposed approaches at 95% significance level.

Modality →	Face		Thermal Face		Palmprint		Palmvein	Fingervein
Scheme↓	CASIA V5	ORL	CASIA NIR	IRIS	CASIA	PolyU	CASIA-MS V1	SDUMLA-HMT
Proposed RS-V1	0.086 ± 0.052	0.095 ± 0.061	0.071 ± 0.015	0.081 ± 0.032	0.069 ± 0.042	0.072 ± 0.048	0.094 ± 0.052	0.092 ± 0.047
Proposed RS-V2	0.132 ± 0.032	0.109 ± 0.045	0.145 ± 0.032	0.120 ± 0.035	0.125 ± 0.041	0.189 ± 0.053	0.117 ± 0.032	0.138 ± 0.041

is greater than 50% for templates belonging to the same subject. It is desirable that *CI* values should be low and much below 50% thereby indicating less correlation and high changeability. For each modality and database 50 transformed databases are generated and used for measuring mutual information content.

Table 6 provides *CI* values between transformed templates for different modalities and databases at 95% significance level. It is observed from Table 6 that *CI* values are low for each variant. This indicates that the proposed approach offers changeability. Also, cross-matching is performed between different combinations of transformed databases. It is described that for high change-

Please cite this article as: H. Kaur, P. Khanna, Random Slope method for generation of cancelable biometric features, Pattern Recognition Letters (2018), https://doi.org/10.1016/j.patrec.2018.02.016

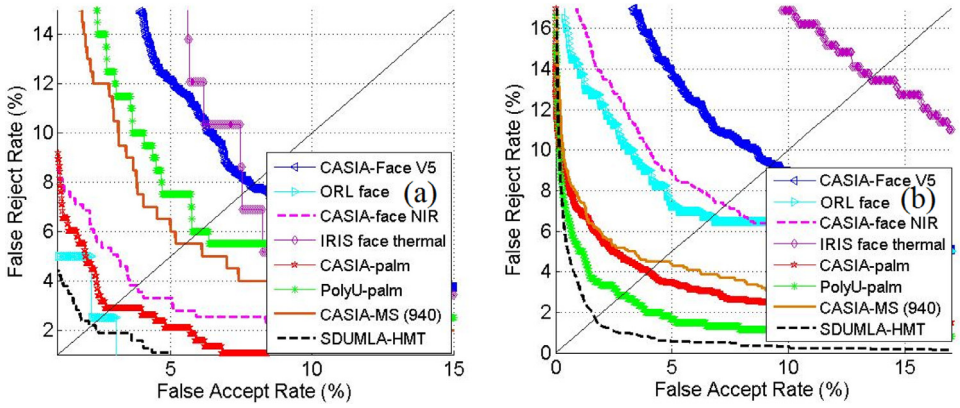

Fig. 7. ROC curves in the worst-case scenario (a) BioConvolving and (b) Random Maxout Permutation transform.

Table 7
Genuine, imposter, and pseudo-imposter distributions along with *EER%* values for the proposed RS-V1 at 95% significance level .

	Modality →	Face		Thermal Face		Palmprint		Palmvein	Fingervein
	Parameter↓	CASIA V5	ORL	CASIA NIR	IRIS	CASIA	PolyU	CASIA-MS V1	SDUMLA-HMT
Genuine	mean (μ_g)	0.563 ± 0.132	0.939 ± 0.124	0.639 ± 0.182	0.955 ± 0.114	0.862 ± 0.158	0.953 ± 0.113	0.993 ± 0.003	0.994 ± 0.004
	variance (σ_g)	0.145 ± 0.012	0.016 ± 0.054	0.158 ± 0.063	0.0451 ± 0.014	0.075 ± 0.021	0.384 ± 0.012	0.016 ± 0.004	0.014 ± 0.006
Impostor	mean (μ_i)	0.283 ± 0.165	0.368 ± 0.163	0.295 ± 0.087	0.369 ± 0.162	0.313 ± 0.121	0.251 ± 0.121	0.304 ± 0.052	0.355 ± 0.041
	variance (σ_i)	0.065 ± 0.025	0.115 ± 0.078	0.083 ± 0.025	0.117 ± 0.112	0.068 ± 0.012	0.059 ± 0.012	0.117 ± 0.071	0.167 ± 0.069
Pseudo-impostor	mean (μ_{pi})	0.351 ± 0.169	0.421 ± 0.129	0.367 ± 0.151	0.440 ± 0.151	0.371 ± 0.114	0.281 ± 0.120	0.361 ± 0.085	0.421 ± 0.079
	variance (σ_{pi})	0.115 ± 0.081	0.154 ± 0.068	0.121 ± 0.058	0.121 ± 0.025	0.109 ± 0.026	0.114 ± 0.051	0.127 ± 0.056	0.142 ± 0.065
Cross match	*EER%*	42.14 ± 3.20	45.36 ± 2.11	42.68 ± 3.25	42.87 ± 2.41	45.68 ± 1.98	46.98 ± 2.14	48.14 ± 1.87	45.89 ± 2.41

Table 8
Genuine, imposter, and pseudo-imposter distributions along with *EER%* values for the proposed RS-V2 at 95% significance level.

	Modality →	Face		Thermal Face		Palmprint		Palmvein	Fingervein
	Parameter↓	CASIA V5	ORL	CASIA NIR	IRIS	CASIA	PolyU	CASIA-MS V1	SDUMLA-HMT
Genuine	mean (μ_g)	0.497 ± 0.124	0.917 ± 0.058	0.601 ± 0.121	0.955 ± 0.112	0.831 ± 0.112	0.953 ± 0.125	0.805 ± 0.120	0.992 ± 0.006
	variance (σ_g)	0.132 ± 0.098	0.141 ± 0.045	0.159 ± 0.85	0.048 ± 0.65	0.134 ± 0.055	0.033 ± 0.021	0.099 ± 0.011	0.023 ± 0.003
Impostor	mean (μ_i)	0.272 ± 0.114	0.301 ± 0.136	0.315 ± 0.121	0.369 ± 0.112	0.267 ± 0.131	0.251 ± 0.122	0.274 ± 0.121	0.395 ± 0.120
	variance (σ_i)	0.065 ± 0.014	0.114 ± 0.058	0.085 ± 0.085	0.118 ± 0.089	0.068 ± 0.014	0.159 ± 0.011	0.098 ± 0.011	0.141 ± 0.012
Pseudo-impostor	mean (μ_{pi})	0.341 ± 0.142	0.351 ± 0.117	0.367 ± 0.152	0.420 ± 0.121	0.314 ± 0.146	0.314 ± 0.124	0.354 ± 0.123	0.451 ± 0.116
	variance (σ_{pi})	0.054 ± 0.021	0.107 ± 0.042	0.114 ± 0.214	0.124 ± 0.052	0.114 ± 0.033	0.043 ± 0.011	0.114 ± 0.020	0.157 ± 0.021
Cross match	*EER%*	45.35 ± 2.14	46.32 ± 1.83	45.25 ± 1.87	45.87 ± 2.14	43.65 ± 2.64	49.23 ± 1.02	45.12 ± 2.14	47.56 ± 1.73

ability the population distribution on cross-matching must fulfill two desirable properties. Firstly, the pseudo-impostor distribution must closely resemble the impostor distribution; and secondly, the genuine distribution must be well separated from the pseudo-impostor distribution [5]. The mean and variances for genuine (μ_g, σ_g), impostor (μ_i, σ_i), and pseudo-impostor scores (μ_{pi}, σ_{pi}) are reported in Tables 7 and 8. It can be observed from the mean and variance that the separability between genuine and pseudo-impostor scores is good, while pseudo-impostor resembles impostor scores. Also, on cross-matching *EER* is high ($\approx$50%) indicating no-match between different transformed templates of same users.

6.3. Non-invertibility

The transformed template *Tf* must be non-invertible even if the user-specific data *RG* and key $\mathcal{K}$ are simultaneously known to an attacker. The transformed template is the sum of normalized slope and intercept vector $Tf(j) = \mathtt{M}'(j) + \mathtt{C}'(j)$. For inverse attack the first problem is to separate the sum to approximate the original vectors $\mathtt{M}'$ and $\mathtt{C}'$, which requires a considerable amount of cryptanalysis. Assuming that multiple copies of transformed template are available and the attacker approximates the normalized vectors $\mathtt{M}'$ and $\mathtt{C}'$, then the next task is to determine the original vectors $\mathtt{M}$ and $\mathtt{C}$. The maximum and minimum values of slope and intercept are required here to estimate the original slope and intercept values. But slope and intercept values are all real numbers $\mathbb{R}$ varying between $(-\infty, -\infty)$. Thus, the inverse operations are very hard and require brute force analysis of very high complexity as the dimensionality of vectors is also very high. Further, even if one is able to access the correct $\mathtt{M}$ and $\mathtt{C}$ by solving or any other attack, knows the random point from key $\mathcal{K}$, and thereby the equation of line *l*. Here also it is computationally hard to determine the original feature point as there are infinite possibilities for this point to lie on the known line *l*. Similarly, for the second variant, the transformed template contains only angle between two lines. Again it is computationally hard to determine original feature points by using angle information and random point.

7. Conclusion

The proposed random slope concept is used for designing two simple yet effective transformation techniques that fulfill the important protection requirements of security, diversity, and revocability. Comparisons are performed using template transformation techniques belonging to different transformation categories and it is found that the proposed approaches give better matching perfor-

Please cite this article as: H. Kaur, P. Khanna, Random Slope method for generation of cancelable biometric features, Pattern Recognition Letters (2018), https://doi.org/10.1016/j.patrec.2018.02.016

mance in the worst-case scenario. The best-case scenario performance for the proposed approaches is also found to be ideal. The non-invertibility is justified for the transformed templates even if the transformation keys are known. The proposed approaches generate revocable templates, reduces dimensionality upto 75%, and performs well while using only simple linear operations to calculate slope and intercepts values. Therefore, random slope based proposed methods can be considered as reliable and competitive template transformation techniques.

Acknowledgment

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

References

[1] AT&T, ORL database of faces, 1994, http://www.cl.cam.ac.uk/.
[2] B. I. Test, CASIA palmprint, 2005, http://www.biometrics.idealtest.org.
[3] B.I. Test, CASIA-MS v1, 2007, http://www.biometrics.idealtest.org.
[4] B.I. Test, CASIA-facev5, 2010, http://www.biometrics.idealtest.org.
[5] Y.J. Chin, T.S. Ong, A.B. Teoh, K. Goh, Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion, Inf. Fusion 18 (2014) 161–174.
[6] S. Cho, A.B. 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.
[7] J.W. Davis, M.A. Keck, A two-stage template approach to person detection in thermal imagery, in: Application of Computer Vision, 2005. WACV/MOTIONS'05 Volume 1. Seventh IEEE Workshops on, IEEE, 2005, pp. 364–369.
[8] R. Dwivedi, S. Dey, R. Singh, A. Prasad, A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping, Comput. Secur. 65 (2017) 373–386.
[9] F. Farooq, R.M. Bolle, T.Y. Jea, N. Ratha, Anonymous and revocable fingerprint recognition, in: Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on, IEEE, 2007, pp. 1–7.
[10] S. Jenisch, A. Uhl, Security analysis of a cancelable iris recognition system based on block remapping, in: Image Processing (ICIP), 2011 18th IEEE International Conference on, IEEE, 2011, pp. 3213–3216.
[11] H. Kaur, P. Khanna, Biometric template protection using cancelable biometrics and visual cryptography techniques, Multimed. Tools Appl. 75 (2016) 16333–16361.
[12] H. Kaur, P. Khanna, Cancelable features using log-gabor filters for biometric authentication, Multimed. Tools Appl. 76 (2017) 4673–4694.
[13] P. Lacharme, E. Cherrier, C. Rosenberger, Preimage attack on biohashing, in: Security and Cryptography (SECRYPT), 2013 International Conference on, IEEE, 2013, pp. 1–8.
[14] C. Lee, J. Kim, Cancelable fingerprint templates using minutiae-based bit-strings, J. Netw. Comput. Appl. 33 (2010) 236–246.
[15] L. Leng, J. Zhang, Palmhash code vs. palmphasor code, Neurocomputing 108 (2013) 1–12.
[16] S.Z. Li, D. Yi, Z. Lei, 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.
[17] E. Maiorana, P. Campisi, A. Neri, Bioconvolving: cancelable templates for a multi-biometrics signature recognition system, in: Systems Conference (SysCon), 2011 IEEE International, IEEE, 2011, pp. 495–500.
[18] J.K. Pillai, V.M. Patel, R. Chellappa, N.K. Ratha, Sectored random projections for cancelable iris biometrics, in: Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on, IEEE, 2010, pp. 1838–1841.
[19] F. Quan, S. Fei, C. Anni, Z. Feifei, Cracking cancelable fingerprint template of ratha, in: Computer Science and Computational Technology, 2008. ISCSCT'08. International Symposium on, IEEE, 2008, pp. 572–575.
[20] N. Ratha, J. Connell, R.M. Bolle, S. Chikkerur, Cancelable biometrics: a case study in fingerprints, in: Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, IEEE, 2006, pp. 370–373.
[21] N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems, IBM Syst. J. 40 (2001) 614–634.
[22] M. Savvides, B.V. Kumar, P.K. Khosla, Cancelable biometric filters for face recognition, in: Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on, IEEE, 2004, pp. 922–925.
[23] A.B. Teoh, A. Goh, D.C. Ngo, Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs, IEEE Trans. Pattern Anal. Mach. Intell. 28 (2006) 1892–1901.
[24] A.B. Teoh, D.N.C. Ling, A. Goh, Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern Recognit. 37 (2004) 2245–2255.
[25] A.B. Teoh, 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.
[26] A.B. Teoh, W.K. Yip, K.A. Toh, Cancellable biometrics and user-dependent multi-state discretization in biohash, Pattern Anal. Appl. 13 (2010) 301–307.
[27] A.B. Teoh, C.T. Yuang, Cancelable biometrics realization with multispace random projections, IEEE Trans. Syst. Man, Cyber. Part B (Cybernetics) 37 (2007) 1096–1106.
[28] H.J. Uhl, E. Pschernig, A. Uhl, Cancelable iris biometrics using block re-mapping and image warping, in: Information Security, Springer, 2009, pp. 135–142.
[29] S. Wang, J. Hu, Design of alignment-free cancelable fingerprint templates via curtailed circular convolution, Pattern Recognit. 47 (2014) 1321–1329.
[30] Y. Wang, Changeable and privacy preserving face recognition, Department of Electrical and Computer Engineering. University of Toronto, 2010 Ph. D. thesis.
[31] Y. Wang, K.N. Plataniotis, An analysis of random projection for changeable and privacy-preserving biometric verification, IEEE Trans. Syst. Man, Cybern. Part B (Cybernetics) 40 (2010) 1280–1293.
[32] 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.
[33] B. Yang, D. Hartung, K. Simoens, C. Busch, Dynamic random projection for biometric template protection, in: Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, IEEE, 2010, pp. 1–7.
[34] M.H. Yang, Face recognition using kernel methods, in: Advances in neural information processing systems, 2002, pp. 1457–1464.
[35] Y. Yin, L. Liu, X. Sun, Sdumla-hmt: a multimodal biometric database, in: Biometric Recognition, Springer, 2011, pp. 260–268.
[36] D. Zhang, Polyu Palmprint Database, Biometric Research Centre, Hong Kong Polytechnic University, 2006 (Online) Available from: (http://www.comp.polyu.edu.hk/biometrics/).
[37] J. Zuo, N.K. Ratha, J.H. Connell, Cancelable iris biometric, in: Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, IEEE, 2008, pp. 1–4.

Please cite this article as: H. Kaur, P. Khanna, Random Slope method for generation of cancelable biometric features, Pattern Recognition Letters (2018), https://doi.org/10.1016/j.patrec.2018.02.016