Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 54 (2015) 661 – 670

Procedia Computer Science

Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

Gaussian Random Projection based Non-invertible Cancelable Biometric Templates

Harkeerat Kaur and Pritee Khanna*

PDPM Indian Institute of Information Technology, Design & Manufacturing Jabalpur 482 005, Madhya Pradesh, India

Abstract

Wide spread use of biometric based authentication implies the need to secure biometric reference data. Various template protection schemes have been introduced to prevent biometric forgery and identity thefts. Cancelable biometrics is a recent approach introduced to address the concerns regarding privacy of biometric data, public confidence, and acceptance of biometric systems. It allows biometric templates to be cancelled and revoked like passwords innumerable times. The work proposes a novel cancelable biometric template generation algorithm using Gaussian random vectors and one way modulus hashing. Instead of using the original templates, the proposed system uses its transformed versions for storing and matching. The approach is tested on face and palmprint biometric modalities. A thorough analysis is performed to analyze the performance, non-invertibility, and distinctiveness of the proposed approach which reveals that the generated templates are non-invertible, easy to revoke, and also deliver good performance.

Peer-review under responsibility of organizing committee of the Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

Keywords: BioHashing; Cancelable biometrics; Gaussian random projections; Modulus hashing; Non-invertible.

1. Introduction

Biometric data is a success for granting access control in various commercial applications such as ATMs, credit cards, bank accounts; government applications such as ID cards, passports, visa, electronic voting, and a number of forensic applications. While the use of biometric templates is easy, convenient and reliable, there are some securities and privacy related issues that need to be addressed:

1. *Impersonation/Identity theft*: Attackers are able to covertly acquire biometrics for example, latent fingerprints and build its physical/digital artifacts to gain illegitimate access.
2. *Sensitivity*: Biometric data reveals a lot of personal and sensitive information about the person.
3. *Security*: Biometric data is being increasingly shared leading to tracing and tracking of users across different databases by matching their reference templates.
4. *Loss of biometric is permanent*: The number of biometric is limited and their compromise/theft can render it useless for the entire lifetime of a user.

*Corresponding author. Tel.: +91-94253-324241.
E-mail address: priteekh@iiitdmj.ac.in

Peer-review under responsibility of organizing committee of the Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)
doi:10.1016/j.procs.2015.06.077

Biometric templates are deployed to increase robustness and security of a system. However at the same time various security and privacy issues are stemming from the use of biometrics. Such situations are leading to a growing gap between the increasing yet conflicting demands of "biometrics for security" and "biometric data protection". To bridge this gap, biometric template protection schemes are required to protect the biometric data/feature, while at the same time maintain capability to identify and verify individuals.

In order to secure the biometric data, it should never be stored in a clear format or the format in which they are obtained from a user. Biometric template protection techniques suggest use of some auxiliary/helper data to transform the reference biometric into a new format such that the above mentioned concerns can be addressed. It is required that, these transformed templates must not compromise the ability to identify/verify individuals, maintain discriminability and intra-user variability, and address various attack scenarios. Cancelable biometrics is an important template protection approach that allows generation of secure and renewable biometric templates which can be cancelled and revoked like passwords innumerable times. This work aims to produce cancelable biometric templates that are non-invertible and deliver a better performance. Cancelability is achieved by projection of biometric template on random matrix whose columns are normally distributed (Gaussian) vectors having zero mean and unit variance followed by a one-way modulus hashing.

Paper is organized as follows. A formal definition of cancelable biometrics, related work and motivation towards the proposed work is provided in Section 2 which is followed by the proposed template transformation approach in Section 3. The experimental results are covered in Section 4 and the work is finally concluded in Section 5.

2. Related Work

To address the above mentioned security and privacy issues Soutar *et al.* (1998) took initiatives to generate renewable and revocable biometric templates[1], and some concrete concepts in this direction were given by Ratha *et al.* (2001)[2]. Cancelable biometrics is defined as "*an intentional and systematically repeated distortions on the biometric data in order to protect the user specific sensitive information*". The biometric template is distorted by subjecting it to transformation functions based on some user defined transformation key or parameter. This transformed template is stored at the time of enrollment as the reference template. At authentication, the query template is distorted using the same transformation function and the user specific parameters, thereafter matched with the reference template. Both storing and matching of templates is performed in transformed domain. It provides high level privacy by allowing multiple templates to be associated with the same biometric data. At every enrollment a different transformation function and/or parameters can be used to generate the protected template. This helps to promote non-linkability of users biometric data stored across various databases. *Biometric salting* and *non-invertible transformations* are two main approaches for template transformation.

BioHashing proposed by Teoh *et al.* (2004) is an instance of biometric salting in which a Tokenized (pseudo) Random Number (TRN) is combined with biometric features to generate BioCodes[3]. In this approach, biometric features are projected on an orthonormal random matrix generated by TRN followed by a two level quantization using thresholding function which results in binary codes called BioCodes. Sutcu *et al.* (2005) proposed robust hashing technique which uses non-invertible transforms, involving nonlinear operations to improve the security of template[4]. However, there exists a tradeoff between discriminability and achieving non-invertibility using this technique. Teoh *et al.* (2006) proposed BioPhasoring to address the invertibility issue[5]. The technique generates a set of complex vectors where the original vectors form the real part and rows of the orthonormal random vector form the imaginary part. This way, BioPhasoring keeps on mixing user specified TRN with the biometric data iteratively and straight forward revocation is possible by token replacement. Secure hashing of dynamic hand signatures using Biophasor mixing and 2^n discretization for cancelable keys generation is given in[6]. Teoh and Yaung (2007) proposed Multispace Random Projection (MRP), a variant of BioHashing to address the stolen token scenario[7]. MRP extracts a fixed length feature vector from the raw biometric template and projects it on a non-invertible random sub-space multiple times. Lumini *et al.* (2007) suggested an improvement in BioHashing by utilizing MRP, different threshold values and fusion of scores[8]. Savvides *et al.* (2004) proposed another instance of biometric salting for generating cancelable face templates using Minimum Average Correlation Energy (MACE) filter and random kernels[9].

Non-invertible transformation functions are usually one way surjective functions that are easy to compute but hard to inverse. These transforms are used to modify the biometric data into a new form within the context of signal or feature domain. A realization of non-invertible transform was proposed by Ratha *et al.* (2007) which suggested that a fingerprint data can be transformed by three different non-invertible transformation functions, Cartesian, polar, and surface folding transformation on the minutiae positions[10]. Tulyakov *et al.* (2005) proposed symmetric hash functions (polynomials) for distorting minutiae information[11]. The hash functions were irreversible because of their one way characteristics, and in case of compromise new templates can be issued by changing the hash functions. Ang *et al.* (2005) proposed key dependent algorithms based on geometric transformations to generate cancelable fingerprint templates[12]. Bout *et al.* (2007) proposed Biotokens, a cryptographically secure technique, which divides the datum into two parts. One part is used for encoding purpose, and the other for approximating a match and support robust distance computation[13]. Farooq *et al.* (2007) presented a concept of generating cancelable bit strings from fingerprint by extracting translational and rotational invariants minutiae triplets[14]. On the same line, Lee *et al.* (2009) proposed minutiae based bit strings to generate cancelable fingerprint templates[15].

Both the above mentioned approaches have their own advantages and disadvantages. BioHashing has been experimentally proven to achieve nearly zero Equal Error Rates (ERR) for various modalities, there by leading to a substantial increase in performance when the system operates in the transformed domain. But, if an adversary gains an access to the transformed template and random data (token stolen), that can generate a coarse approximation of the original template as the process is invertible. Hence, the security of the data is compromised and performance regresses in a stolen token scenario. The security of the non-invertible transformations lies in the fact that even if the token and/or the transformed template are stolen, it is computationally hard for an adversary to obtain the original biometric data. However, many a times non-invertible transforms tends to compromise discriminability of the transformed templates there by decrease in performance. To maintain a balance between discriminability and non-invertiblity is a major challenge while designing template transformation techniques. The work is motivated towards designing a transformation approach such that the templates are easy to revoke, difficult to invert and does not degrade performance.

3. Template Transformation

This work produces cancelable biometric templates by projection of biometric template on random matrix whose columns are normally distributed (Gaussian) vectors having zero mean and unit variance followed by a one-way modulus hashing. The properties of Gaussian projection and step wise approach are discussed in the following sections.

3.1 Gaussian random projection

Random projection is a powerful dimensionality reduction tool. Its key concept arises from Johnson and Lindenstrauss lemma (JL lemma) which states that a set of d points in a high dimensional Euclidean space can be mapped down onto a k-dimensional subspace ($k \geq O(logd/\epsilon^2)$), such that the distances between the points are approximately preserved (i.e., not distorted more than a factor of $(1 \pm \epsilon$, for $0 < \epsilon < 1)$[16]. Using matrix notation, the original data can be represented as $X_{d\times N}$, which can be considered a set of N observations of dimension-d. Its projection on a k- dimensional random subspace ($k \ll d$) is denoted as

$$X^{RP}_{k\times N} = R_{k\times d} X_{d\times N}, \tag{1}$$

where R is random $k \times d$ matrix whose columns has unit norm and X^{RP} is the projection of X in lower dimensional subspace. The effect to which pair-wise distances between points before and after projection are preserved depends upon the projection vectors $r_i \in R$. The essential property of the projection matrix in JL lemma is that its column vectors $r_i \in R$ are required to be orthogonal to each other. Gram Schmidt orthogonalization process is a technique that is usually applied to transforms the columns of a random vector into orthogonal ones. Achieving orthogonality is a very computationally expensive process.

To improve the computation costs of dimensionality reduction algorithms various variants and improvements are proposed by researchers[20]. In a research on approximating nearest-neighbor in a high dimensional Euclidean space,

Indyk and Motwani noted that the condition of orthogonality can be dropped while using random projections. To prove it, they computed a random projection matrix whose column entries are independent random variables with the standard normal distribution $N(0, 1)$. By using the properties of normal distribution, they proved that the projection x^{RP} of a unit vector $x \in \Re^d$ has the chi-square distribution with k-degrees of freedom, and tail estimates for this distribution can be used to prove that the pair-wise distance between any two points is not distorted by a factor more than $(1 \pm \epsilon)$[17]. Dasgupta proposed a similar construction of random projection matrix in which each row is also rescaled to a unit vector. Using elementary probabilistic techniques they proved that the preservation of pair-wise distance before and after projection[18]. Projection on normally distributed (or Gaussian distributed) random vectors, having zero mean and unit variance is a distance preserving mapping with less computation costs. According to the properties of normally distribution, the linear projection of a Gaussian remains Gaussian. Hence, a mixture of high dimensional Gaussians onto a single vector will be producing a mixture of univariate normally distributed variables. For a deeper insights and mathematical proofs the following papers are suggested to be referred[17,19,21].

3.2 Proposed transformation algorithm

The following operations are performed to generate a cancelable template:

Step 1. A raw biometric grayscale image is acquired and its columns are stored as a set of N, d-dimensional vectors, $I \in \Re^d$. In matrix form it can be represented as $I_{d\times N}$.

Step 2. The image is preprocessed by extraction of region of interest from the sample followed by illumination enhancement. The effect of uniform illumination with linear scale of lighting intensity can be adjusted by simple gray-level histogram equalization. Histogram equalization uniformly distributes the intensity values of the image and produces an enhanced image of better contrast and increased dynamic range.

Step 3. Generate a set of k-dimensional normally distributed random vectors having zero mean, unit variance and values ranging between $[-1, 1]$ such that $\{r_i \in \Re^k | i = 1, \ldots, d\}$. The vectors r_i are column wise concatenated to produce the random projection matrix $R_{k\times d}$.

Step 4. Project the acquired biometric data image matrix I on the Gaussian random matrix R. Its projection on a k-dimensional random subspace ($k \ll d$) is denoted as given in Eq. (1). In terms of matrices it can be expressed as

$$\begin{bmatrix} I^{RP}_{1,1} & \cdots & I^{RP}_{1,N} \\ \cdot & \cdots & \cdot \\ I^{RP}_{k,1} & \cdots & I^{RP}_{k,N} \end{bmatrix} = \begin{bmatrix} R_{1,1} & \cdots & R_{1,d} \\ \cdot & \cdots & \cdot \\ R_{k,1} & \cdots & R_{k,d} \end{bmatrix} \times \begin{bmatrix} I_{1,1} & \cdots & I_{1,N} \\ \cdot & \cdots & \cdot \\ I_{d,1} & \cdots & I_{d,N} \end{bmatrix} \tag{2}$$

Step 5. Apply low pass Gaussian filter to smoothen the image. A Gaussian filter smoothes an image by calculating weighted average in a filter box and attenuates high varying intensity components.

Step 6. The column wise mean of the projected matrix I^{RP} is calculated and stored in a vector M, $M \in \Re^k$. The elements of vector M are transformed are transformed as:

$$M(j) = \min\{256, abs(\lfloor M(j) \rfloor) + 1\} \tag{3}$$

where *abs* is absolute value function and $\lfloor\rfloor$ represents greatest integer function.

Step 7. Using vector M, compute modulus separately for each j^{th} column of the projected template as:

$$I^T(:, j) = I^{RP}(:, j) \mod M(j), \tag{4}$$

where j varies from 1 to N and the total number of rows and columns being k and N respectively. After computing the transformed template I^T, the vector M is discarded.

Step 8. Approximate the fractional values of the elements of I^T towards positive infinity. Since the maximum value of modulus is 256, the resultant transformed template after approximation has integral values ranging from 0 to 255.

Block diagram of the proposed algorithm is given in Fig. 1. The matching is performed in the transformed domain by calculating Euclidean distances between the extracted vectors of the transformed reference and query biometric template. In case of compromise of the templates, new ones can be generated by changing the token/projection matrix.

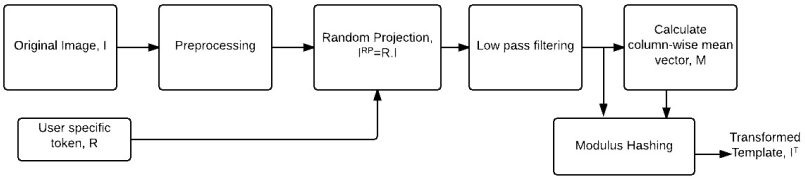

Fig. 1. Block diagram of the proposed approach.

4. Experimental Results and Discussion

An experimental study is performed to study various aspects of the proposed system such as matching performance and distinctiveness of the transformed templates. As non-invertibility is an essential characteristic of cancelable template, the stolen token scenario is also analyzed to determine the strength against invertibility attacks.

4.1 Databases used for experimentation

The performance is evaluated on two different biometric modalities, i.e., face and palmprint. For face modality three different standard facial databases, ORL, Indian face database, and Extended Yale Face Database B are used. ORL[22] is an expression variant database consisting of 40 subjects with 10 images per subject capturing different facial expressions . Extended YALE face database[23] is an illumination variant database containing 64 near frontal images for 38 subjects under various illumination conditions. Out of it only 10 images per subject are selected with uniform illumination having linear scale of lighting intensity variations. The Indian face database[24] is a collection of 61 subjects, 39 males and 22 females with 11 images per subjects collected by IIT Kanpur for different orientation of face, eyes, and emotions on face. For each database, 3 images are randomly selected for training database and 6 images for test database. To study the functional performance of the proposed system on palmprint image templates CASIA[25] and PolyU[26] databases are also used. CASIA contains 5,239 hand images captured from 301 subjects corresponding to 602 palms. PolyU database includes 600 images from 100 individuals, with 6 palmprint images from each subject. For these palmprint databases, 2 images for training and 4 images for testing purposes are randomly selected after extraction of region of interest[27].

4.2 Performance evaluation on facial and palmprint image templates

The performance is evaluated on Equal Error Rates (ERR) and Decidability Index (DI). Decidability Index (DI) is defined as the normalized distance between means of Genuine (μ_G) and Imposter distributions (μ_I). DI index 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

$$DI = \frac{|\mu_G - \mu_I|}{\sqrt{(\sigma_G^2 + \sigma_I^2)/2}} \tag{5}$$

To establish a bench mark for comparison, the performance of the system is calculated when the templates are stored and matched in the original format (without any transformation) using two most common techniques Principal Component Analysis (PCA)[28] and Linear Discriminant Analysis (LDA)[29,30]. All the original image templates are resized to $d \times N$ pixels, where $d = N = 128$. The projection matrix is a set of d column vectors which are generated as normally distributed pseudorandom numbers in the range of $[-1, 1]$ having zero mean and unit variance. The column vector r_i belongs to k-dimensional Euclidean space, $r_i \in \Re^k$ and let initially $k = d = 128$. The matrices are square and on transformation the dimensions of the template is same as that of the original, i.e., 128×128 pixels.

Table 1 and 2 provides ERR and DI for matching performance in original domain and transformed domain for face and palmprint respectively. For both the modalities in comparison to the original domain, ERR values in transformed domain are very low and near to zero. Similarly, DI increases in transformed domain indicating better separability

Table 1. Matching performance for face databases.

	Original templates				Transformed templates			
	PCA		LDA		PCA		LDA	
Database	ERR	DI	ERR	DI	ERR	DI	ERR	DI
ORL	12.44%	1.897	4.2%	2.542	0.00%	5.254	0.00%	6.511
YALE	32.5%	0.855	11.7%	1.698	0.03%	4.568	0.08%	5.936
Indian face	10.6%	1.639	8.5%	1.546	0.12%	4.591	0.00%	5.293

Table 2. Matching performance for palmprint databases.

	Original templates				Transformed templates			
	PCA		LDA		PCA		LDA	
Database	ERR	DI	ERR	DI	ERR	DI	ERR	DI
PolyU	9.2%	1.22	2.3%	1.54	0.21%	4.582	0.08%	5.939
CASIA	4.3%	1.85	0.8%	2.0	0.19%	4.685	0.02%	5.845

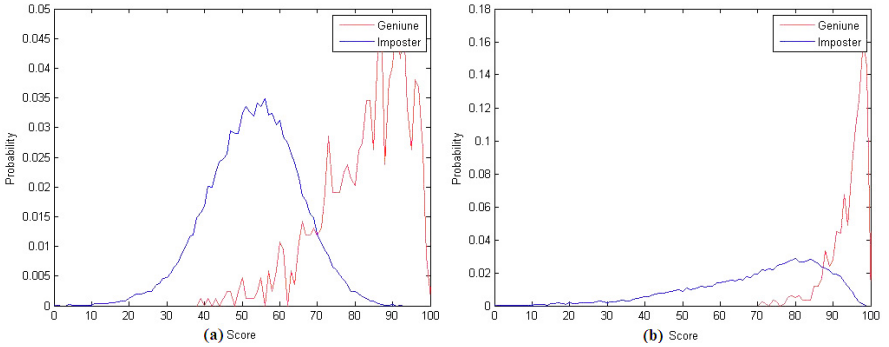

Fig. 2. Population distribution for original templates of ORL face database, (a) PCA based matching; (b) LDA based matching.

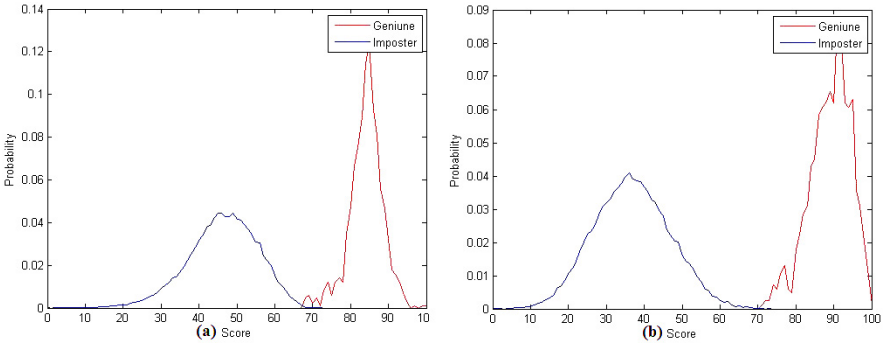

Fig. 3. Population distribution for transformed templates of ORL face database, (a) PCA based matching; (b) LDA based matching.

between templates in transformed domain. Figures 2 and 3 represent genuine and imposter population distribution curves for ORL database before and after transformation respectively. Figures 4 and 5 depict genuine and imposter population distribution curves for PolyU database before and after transformation respectively. It is seen in Figs. 3 and 5 that the separation between genuine and imposter population increases significantly after applying the proposed transformation.

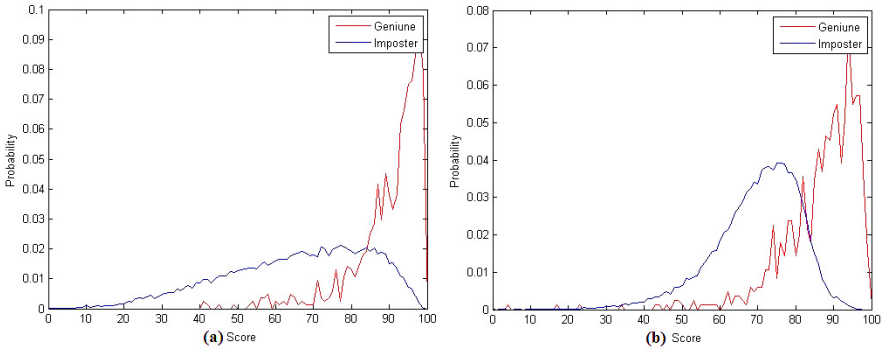

Fig. 4. Population distribution for original templates of PolyU palmprint database, (a) PCA based matching; (b) LDA based matching.

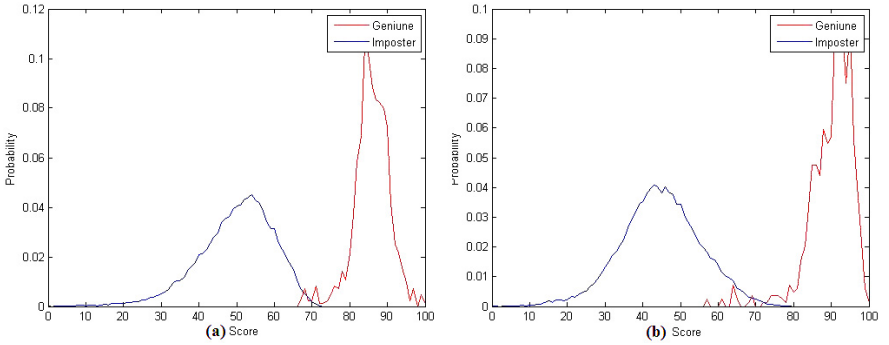

Fig. 5. Population distribution for transformed templates of PolyU palmprint database, (a) PCA based matching; (b) LDA based matching.

The increase in performance is due to the fact that random projection increases inter-user variations. For each user the projection matrix is different, and hence it is possible to obtain a clear separation between the genuine population and the imposter population.

4.3 Invertibility analysis

Consider the stolen token scenario, when the transformed template I^T and the key projection matrix R are available simultaneously. The key projection matrix R is a square matrix, hence its inverse exists.The inverse operation (decryption) requires projection of the transformed template over the inverse of key matrix computed as

$$I^{\text{inv\_proj}} = R^{-1} * I^T \tag{6}$$

The next step requires an attacker to have the exact knowledge of the values over which modulus is computed for each column, i.e., the mean vector M. Since the vector is discarded after transforming the template it is not available with the attacker. Yet, we consider a scenario where the exact vector M is also available with the attacker. The inverse template is obtained by computing modulus for the j^{th} column of $I^{\text{inv\_proj}}$ using the j^{th} value of vector M as

$$I^{\text{rec}} = I^{\text{inv\_proj}}(:, j) \mod M(j), \tag{7}$$

where j varies from 1 to N, the total number of rows and columns are d and N respectively. Combined Eq. (2) and (4), and Eq. (6) and (7) are analogous to the Hill cipher encryption and decryption equations, respectively. Hill cipher is a symmetric encryption algorithm and works on blocks of data. To encrypt a block of plaintext P of size $n \times 1$, a key matrix K of size $n \times n$ is required which has non-negative integral values ranging from 0 to $N - 1$ where $N = 26$

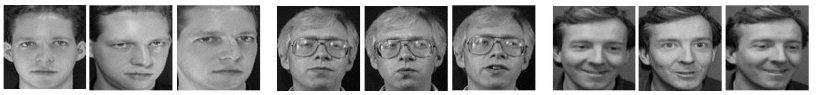

Fig. 6. Samples of a few original templates.

Fig. 7. Samples of transformed templates relative to templates shown in Fig. 6.

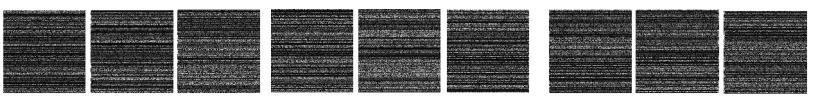

Fig. 8. Samples of inverted templates obtained from the transformed templates shown in Fig. 7.

for alphabets and $N = 256$ for gray level images. The ciphertext C is obtained by matrix multiplication of K over P followed by computing the modulus over N, represented as

$$C = (K * P) \mod N \tag{8}$$

The determinant of the encryption matrix K must be relatively prime to N, where $C_1 = (K_{1,1} * P_1 + \cdots + K_{1,n} * P_n) \mod N$ and $C_n = (K_{n,1} * P_1 + \cdots + K_{n,n} * P_n) \mod N$. To decrypt the ciphertext, inverse of the key matrix K^{-1} is required to be computed. The equation for decryption process can be written as:

$$P = (K^{-1} * C) \mod N \tag{9}$$

To perform decryption it is necessary that the key matrix must be invertible, which essentially requires it to be a square matrix and $gcd(\det(K) \mod N, N) = 1$. Here gcd is the greatest common divisor and $\det(K)$ denotes the determinant of K. Though the key matrix might be invertible, the recovered/decrypted information might still suffer from the loss of information. To ensure a perfectly lossless recovery of data after decryption, it is necessary that all elements of the inverse key matrix, K^{-1} should contain non-negative integral values.

In our case the key matrix comprises of normally distributed column vectors whose elements have rational values ranging between $[-1, 1]$. Thus its inverse would always possess rational entries making the decryption operation suffer from serious loss of information content. When a grayscale image matrix having non-negative values between [0, 255] is projected on normally distributed random matrix $[-1, 1]$, the resulting matrix is a set of negative and non-negative fractional values which are later subjected to modulus operation. When the transformed matrix is subjected to decryption operation the information is not recoverable. Figs. 6, 7 and 8 illustrate the samples of actual image templates, their transformed versions, and their recovered templates, respectively. The recovered templates are lousy and most of the original information is not recovered.

4.4 Histogram analysis

Histograms are plotted to analyze the intensity distribution of matrix elements at various stages. The histogram of the original image matrix, the projected matrix, the transformed matrix, and the recovered matrix for a sample biometric face image template is depicted in Fig. 9. On comparing the histograms of the recovered and the original images it is found that they are completely different from each other. This indicates that the recovered template does not reveal any information about the original image.

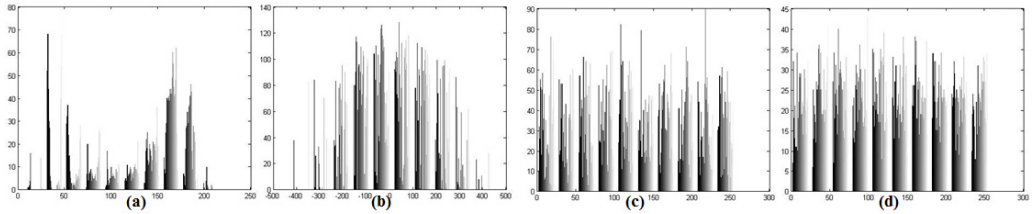

Fig. 9. Histograms of, (a) Original image, I; (b) Projected image, I^{RP}; (c) Transformed image I^{T}; (d) Recovered image I^{rec}.

4.5 Distinctiveness analysis

The ability to generate various transformed template by changing the transformation parameter is the basis of achieving revocability and diversity.The correlation coefficients is calculated among various transformed templates of biometric samples having different transformation matrix (random projection matrix R) using Eq. (10)

$$C_r(I_1, I_2) = \frac{\sum\sum(I_1 - \bar{I_1})(I_2 - \bar{I_2})}{\sqrt{(I_1 - \bar{I_1})^2 + (I_2 - \bar{I_2})^2}}, \tag{10}$$

where $\bar{I_1}$, $\bar{I_2}$ represents the mean of images I_1, I_2 respectively. At first, correlation coefficients are calculated between transformed templates belonging to same subject and transformed templates belonging to different subjects keeping fixed and unique projection matrix for each subject. It is found that correlation coefficients ranges from 0.5 to 0.75 for different transformed templates belonging to same subject indicating similarity. The correlation coefficients between templates belonging to different subjects is nearly zero, indicating that there does not exists any correlation between transformed templates of different subjects.

In the next case, the biometric image samples are kept fixed and different transformed templates are created by changing the random matrix. The correlation coefficients between various transformed versions of the same biometric sample is calculated and found to be nearly zero, indicating no correlation.

4.6 Comparison with BioHashing

Essentially both the techniques deliver comparable performance i.e., nearly zero EER. Apart from the nature of the random projection matrices, i.e., orthonormal in BioHashing and Gaussian (normally distributed) in the proposed approach, there are some other essential differences. While BioHashing only generates binary valued codes, the proposed template possesses integral values between [0, 255]. BioHashing claims non-invertibility by performing binarization, is a many to one mapping on the basis of a fixed threshold value. However, recent attacks have proved that in stolen token scenario, when the transformed template and the projection matrix is simultaneously available, it is possible to invert the process and generate an approximate pre-image of the original biometric[31,32]. Hence, it is practically an invertible process. On the other hand the proposed approach is non-invertible and maintains performance in stolen token scenarios as proved in the above sub-sections.

5. Conclusion

The transformed templates produced in the proposed approach deliver better performance as compared to their original counterparts. Thus, the proposed approach successfully meets an important requirement of achieving good recognition rates in the transformed domain. Non-invertiblity being an important requirement is also thoroughly analyzed and the transformed templates are not found to reveal any original information when subjected to inverse operations. Revocability and diversity is achieved by simply changing the random projection matrix. However, the complexity is increased due to the involvement of matrix multiplication operations.

References

[1] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B. V. Kumar, Biometric Encryption using Image Processing, In *Photonics West'98 Electronic Imaging, International Society for Optics and Photonics*, pp. 178–188, (1998).

[2] N. K. Ratha, J. H. Connell and R. M. Bolle, Enhancing Security and Privacyin Biometrics – Based Authentication Systems, *IBM Systems Journal*, vol. 40(3), pp. 614–634, (2001).

[3] 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(11), pp. 2245–2255, (2004).

[4] Y. Sutcu, H. T. Sencar and N. Memon, A Secure Biometric Authentication Scheme Based on Robust Hashing, In *Proceedings of the 7th Workshop on Multimedia and Security ACM*, pp. 111–116, (2005).

[5] A. B. J. Teoh and D. C. L. Ngo, Biophasor: Token Supplemented Cancellable Biometrics, In *IEEE 9th International Conference on Control, Automation, Robotics and Vision, ICARCV'06*, pp. 1–5, (2006).

[6] Y. W. Kuan, A. B.Teoh and D. C. Ngo, Secure Hashing of Dynamic Hand Signatures using Wavelet – Fourier Compression with Biophasor Mixing and 2n discretization, *EURASIP Journal on Applied Signal Processing*, vol. (1), pp. 32–32, (2007).

[7] A. Teoh and C. T. Yuang, Cancelable Biometrics Realization with Multispace Random Projections, *IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics*, vol. 37(5), pp. 1096–1106, (2007).

[8] A. Lumini and L. Nanni, An Improved Biohashing for Human Authentication, *Pattern Recognition*, vol. 40(3), pp. 1057–1065, (2007).

[9] M. Savvides, B. V. Kumar and P. K. Khosla, Cancelable Biometric Filters for Face Recognition, In *Proceedings of the 17th International Conference on Pattern Recognition, ICPR 2004*, vol. 3, IEEE; pp. 922–925, (2004).

[10] N. Ratha, J. Connell, R. M. Bolle and S. Chikkerur, Cancelable Biometrics: A Case Study in Fingerprints, In *18th International Conference on Pattern Recognition, ICPR 2006*, vol. 4, IEEE, pp. 370–373, (2006).

[11] S. Tulyakov, F. Farooq and V. Govindaraju, Symmetric Hash Functions for Fingerprint Minutiae, In *Pattern Recognition and Image Analysis*, Springer, pp. 30–38, (2005).

[12] R. Ang, R. Safavi-Naini and L. McAven, Cancelable Key-Based Fingerprint Templates, In *Information Security and Privacy*, Springer, pp. 242–252, (2005).

[13] T. E. Boult, W. J. Scheirer and R. Woodworth, Revocable Fingerprint Biotokens: Accuracyand Security Analysis, In *IEEE Conference on Computer Vision and Pattern Recognition, CVPR'07*, IEEE; pp. 1–8, (2007).

[14] F. Farooq, R. M. Bolle, T. Y. Jea and N. Ratha, Anonymous and Revocable Fingerprint Recognition, In *IEEE Conference on Computer Vision and Pattern Recognition, CVPR'07*, IEEE, pp. 1–7, (2007).

[15] C. Lee and J. Kim, Cancelable Fingerprint Templates using Minutiae-Based Bit-Strings, *Journal of Network and Computer Applications*, vol. 33(3), pp. 236–246, (2010).

[16] S. Dasgupta and A. Gupta, An Elementary Proof of the Johnson-Lindenstrauss Lemma, *International Computer Science Institute, Technical Report*, pp. 99–006, (1999).

[17] P. Indyk and R. Motwani, Approximate Nearest Neighbors: Towards Removing the Curse of Dimensionality, In *Proceedings of the Thirtieth Annual ACM Symposium on Theoryof Computing, ACM*, pp. 604–613, (1998).

[18] S. Dasgupta, Learning Mixtures of Gaussians, In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, IEEE, pp. 634–644, (1999).

[19] E. Bingham and H. Mannila, Random Projection in Dimensionality Reduction: Applications to Image and Text Data, In *Proceedings of the Seventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM*, pp. 245–250, (2001).

[20] J. Matoušek, On Variants of the Johnson–Lindenstrauss Lemma, *Random Structures & Algorithms*, vol. 33(2), pp. 142–156, (2008).

[21] B. Klartag and S. Mendelson, Empirical Processes and Random Projections, *Journal of Functional Analysis*, vol. 225(1), pp. 229–245, (2005).

[22] ORLface Database, AT&T Laboratories Cambridge; http://www.cl.cam.ac.uk/.

[23] Yaleface Database, Center for Computational Vision and Control at Yale University, http://cvc. yale.edu/projects/yalefaces/yalefa/.

[24] The Indianface Database, IIT Kanpur, http://vis-www.cs.umas.edu/.

[25] CASIA Palmprint Database, Biometrics Ideal Test, http://biometrics.idealtest.org/downloadDB/.

[26] PolyU Palmprint Database, The Hong Kong Polytechnic University, http://www4.comp.polyu.edu.hk/b̃iometrics/.

[27] H. Kekre, T. Sarode and R. Vig, An Effectual Method for Extraction of roi of Palmprints, In *Communication, Information & Computing Technology (ICCICT), 2012 International Conference on IEEE*, pp. 1–5, (2012).

[28] M. A.Turk and A. P. Pentland, Face Recognition using Eigenfaces, In *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91, IEEE Computer Society Conference on IEEE*, pp. 586–591, (1991).

[29] M. S. Bartlett, J. R. Movellan and T. J. Sejnowski, Face Recognition by Independent Component Analysis, *Neural Networks, IEEE Transactions on*, vol. 13(6), pp. 1450–1464, (2002).

[30] T. Connie, A. Teoh, M. Goh and D. Ngo, Palmprint Recognition with pca and ica, In *Proc. Image and Vision Computing, New Zealand*, (2003).

[31] P. Lacharme, E. Cherrier and C. Rosenberger, Preimage Attack on Biohashing, In *International Conference on Security and Cryptography (SECRYPT)*, (2013).

[32] Y. Lee, Y. Chung and K. Moon, Inverse Operation and Preimage Attack on Biohashing, In *Computational Intelligence in Biometrics: Theory, Algorithms and Applications, CIB, IEEEWorkshop on IEEE*, pp. 92–97, (2009).