Cancelable Biometrics Using Hadamard Transform and Friendly Random Projections

Harkeerat Kaur and Pritee Khanna

Abstract Biometrics based authentication increases robustness and security of a system, but at the same time biometric data of a user is subjected to various security and privacy issues. Biometric data is permanently associated to a user and cannot be revoked or changed unlike conventional PINs/passwords in case of thefts. Cancelable biometrics is a recent approach which aims to provide high security and privacy to biometric templates as well as imparting them with the ability to be canceled like passwords. The work proposes a novel cancelable biometric template protection algorithm based on Hadamard transform and friendly random projections using Achlioptas matrices followed by a one way modulus hashing. The approach is tested on face and palmprint biometric modalities. A thorough analysis is performed to study 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.

Keywords Cancelable biometrics · Hadamard transform · Random projections · Non-invertible

1 Introduction

Biometrics based authentication is a significant component of current and emerging identification technologies. Typical examples are physical and online access control systems in government organizations, banks, and other commercial uses. There are various security and privacy issues stemming from the widespread usage of biometric systems that needs to be addressed. Ratha et al. [1] identified eight points at

H. Kaur (✉) · P. Khanna
PDPM Indian Institute of Information Technology,
Design and Manufacturing, Jabalpur, Madhya Pradesh, India
e-mail: harkeerat.kaur@iiitdmj.ac.in

P. Khanna
e-mail: pkhanna@iiitdmj.ac.in

B. Raman et al. (eds.), *Proceedings of International Conference on Computer Vision and Image Processing*, Advances in Intelligent Systems and Computing 460,
DOI 10.1007/978-981-10-2107-7_5

which a generic biometric system can be attacked. However, amongst many identified issues, stolen biometric scenario where an imposter is able to spoof by providing a stolen biometric sample of the genuine user, is the current threat to deal with. Database attacks leads to permanent template compromise, where an attacker uses the stored biometric data to obtain illegitimate access. As biometric data is being increasingly shared among various applications, cross matching of different databases may be performed to track an individual. Unlike passwords or PINs, biometric templates cannot be revoked on theft. Biometric template are permanently associated with a particular individual and once compromised, it will be lost permanently. Moreover, the same template is stored across different application databases which can be compromised by cross-matching attack. Template data once compromised for one application renders it compromised and unsafe for all other applications for entire lifetime of the user. The concept of cancelable biometrics addresses these concerns. Instead of original biometrics, it uses its transformed versions for storing and matching purposes. In case of any attack, the compromised template can be revoked and new transformed versions can be easily generated.

The objective of this work is to generate biometric templates which can canceled like passwords while at the same time provide non-repudiation and perform like generic biometric templates. Cancelability is achieved by first subjecting the image to Hadamard transformation (HT) and then projecting it on a random matrix whose columns are independent vectors having values –1, +1, or 0 with probabilities 1/6, 1/6, and 2/3, respectively. The sample is then subjected to inverse HT followed by a one-way modulus hashing on the basis of a vector computed in Hadamard domain. The organization of the paper is as follows. A formal definition of cancelable biometrics and related works is provided in Sect. 2. It is followed by the proposed template transformation approach explained in Sect. 3. The experimental results are covered in Sect. 4, and finally the work is concluded in Sect. 5.

2 Cancelable Biometrics

Cancelable biometrics is an important template protection scheme which is based on intentional and systematic repeated distortions of biometric data to protect user specific sensitive information. Unlike other protection schemes like cryptosystems and steganography, the original biometric is never revealed and system operates on transformed data. The biometric data is transformed using some user-specific parameters and transformed template is registered. At authentication, the query template is distorted using similar constraints, thereafter matched with the reference template. Same biometric can be enrolled differently by changing the transformation function and/or parameters for its use in different applications. This prevents cross matching attacks and leads to increase in overall security, privacy, and non-linkability of biometric data. *Biometric salting* and *non-invertible transformation* are two main template transformation approaches.

Teoh et al. (2004) proposed BioHashing which salts biometric features by projecting them on user-specific random matrices (Random Projection) followed by thresholding to generate binary codes. BioHashing becomes invertible if the binary codes and user-specific random matrices are compromised and pre-image attack can be simulated to recover the original data [2]. Sutcu et al. (2005) proposed a nonlinear transformation based salting technique known as robust hashing [3]. The technique is non-invertible but the hashed templates tend to compromise on discriminability. Teoh et al. (2006) proposed BioPhasoring which iteratively mixes biometric features with user-specific random data in a non-invertible fashion without losing discriminability [4]. To address the invertibility of Biohashing, Teoh and Yaung (2007) proposed salting techniques which involve Multispace Random Projections (MRP) [5]. Further, Lumini et al. (2007) combined Multispace Random Projections, variable thresholding, and score level fusions to enhance performance [6].

Non-invertible transformations are many-to-one functions that easily transform biometric data into a new mapping space. Ratha et al. (2007) generated non-invertible cancelable fingerprint templates by distorting minutiae features using Cartesian, polar, and surface folding transformation functions [7].Tulyakov et al. (2005) distorted minutiae features using polynomial based one way symmetric hash functions [8]. Ang et al. (2005) generated cancelable minutiae features using key dependent geometric transformation technique [9]. Bout et al. (2007) generated revocable biometric based identity tokens from face and fingerprint templates by using one way cryptographic functions. The technique separates data into two parts, such that the integer part is used for encryption and the fractional part is used for robust distance computations [10]. Farooq et al. (2007) and Lee et al. (2009) extracted rotation and translation invariant minutiae triplets to generate cancelable bit string features [11].

Each of the above mentioned approaches have their own advantages and disadvantages. BioHashing and other salting techniques are effective but are subjective to invertibility. Also their performance degrades considerably in stolen token scenario. Non-invertible transforms tends to compromise discriminability of transformed biometric in order to achieve irreversibility which degrades the performance. It is imperative to maintain a balance between non-invertiblity, discriminability, and performance for a cancelable biometric technique. This work is motivated towards designing a transformation approach such that the templates are easy to revoke, difficult to invert, and maintains performance in stolen token scenario.

3 Template Transformation

Along with the basics of Hadamard transform and Random Projection, proposedtemplate transformation technique is discussed here.

3.1 Hadamard Transform

Hadamard transform (HT) is non-sinusoidal and orthogonal transformation which offers significant computational advantage over Discrete Fourier Transform (DFT) and Discrete Cosine Transform (DCT). It decomposes an arbitrary input signal into a set of Walsh functions. Walsh functions are orthogonal, rectangular and can be generated using Kroneckers product of the Hadamard matrices. Hadamard matrix of order n is the $N \times N$ matrix, where $N = 2^n$, generated by the iteration rule given as

$$H_n = H_1 \otimes H_{n-1} \tag{1}$$

$$H_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2}$$

Since the elements of the Hadamard matrix (H_n) are real containing only +1 and –1, they are easy to store and perform computations. H_n is an orthogonal matrix. HT has good energy packing properties, but it cannot be considered a frequency transform due to its non-sinusoidal nature. The sign change along each row of H_n is called sequence which exhibits characteristics like frequency. HT is fast as its computation requires only simple addition and subtractions operations. It can be performed in $O(Nlog_2N)$ operations. For a 2-D vector I of dimensions $N \times N$ where $N = 2^n$, the forward and inverse transformations are performed using Eqs. 3 and 4, respectively.

$$F = (H_n \times I \times H_n)/N \tag{3}$$

$$I = (H_n \times F \times H_n)/N \tag{4}$$

3.2 Random Projection

Random projection is a widely used dimensional reduction technique based on Johnson and Lindenstrauss lemma (JL lemma). JL lemma states that a set of d points in a high dimensional Euclidean space can be mapped down onto a k-dimensional subspace ($k \geq O(logd/\epsilon^2)$, where $0 < \epsilon < 1$), such that the distances between any two points before and after projection is approximately preserved [12]. The effect to which pair-wise distances between points before and after projection are preserved depends upon the projection vectors. The essential property of the projection matrix R used 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 transform the columns of a random vector into orthogonal ones. Achieving orthogonality is computationally expensive.

To reduce the computation costs of dimensionality reduction algorithms various variants and improvements are proposed by researchers [13]. In a research on

approximating nearest-neighbor in a high dimensional Euclidean space, Indyk and Motwani claimed that column vectors of projection matrix need not to be orthogonal to each other while using random projections [14]. They proved that projection on a random matrix whose column entries are independent random variables with the standard normal distribution having zero mean and unit variance is a distance preserving mapping with less computation cost. Dasgupta proposed a similar construction of random projection matrix in which each row is also rescaled to a unit vector and proved its distance preserving ability using elementary probabilistic techniques [15]. Achlioptas replaced the Gaussian distribution with a computationally inexpensive and upto three times faster projection matrix, A, whose columns are independent vectors defined as [16]

$$A(i,j) = \sqrt{3}\begin{cases} +1, \text{with probability } 1/6; \\ 0, \text{ with probability } 2/3; \\ -1, \text{with probability } 1/6. \end{cases} \tag{5}$$

This allows computation of projected data using simple addition and subtraction operations and is well suited for database environments. Detailed proofs and deeper insights about the distance preservation property of projections using Achiloptas matrix can be found in [13, 16, 17].

3.3 Proposed Transformation Algorithm

A raw biometric grayscale image I is acquired and preprocessed by applying histogram equalization for illumination enhancement followed by extracting region of interest. For the sake of applying HT the dimensions of preprocessed image are kept of the order of power of 2, here $N \times N$ pixels, $N = 128$. Image I^H is obtained by applying forward HT to the preprocessed image using Eq. 3, where size of H_n is $N \times N, N = 128$. A user specific random matrix R of dimensions $d \times k$ is generated using Eq. 5 where $d = k = 128$. Randomness is introduced by projecting the forward HT image I^H on the matrix R as

$$I^{RP} = I^H \times R/\sqrt{k} \tag{6}$$

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

$$M(j) = \max\{256, \text{abs}(\lfloor M(j) \rfloor) + 1\} \tag{7}$$

where *abs* is absolute value function. Exploiting the energy compaction property of HT, the coefficients confining to the upper left triangle which gives the basic details of the image are retained and rest are discarded by equating them to zero. On the

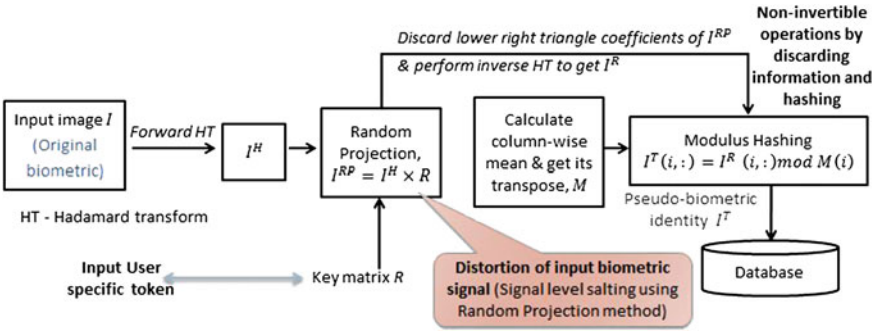

Fig. 1 Block diagram of the proposed approach

resultant, inverse HT is performed using Eq. 4 to obtain I^R. Modulus for each ith row of I^R is separately calculated using vector M.

$$I^T(i,:) = I^{RP}(i,:) \bmod M(i) \tag{8}$$

where i 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. Overall I^T can be written as

$$I^T = (H_n \times \left((H_n \times I \times H_n) \times R\right) \times H_n) \bmod M \tag{9}$$

Approximate 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 possess integral values between 0 to 255. Figure 1 depicts the block diagram of the proposed approach. Discriminative features are extracted from the transformed template I^T using Linear Discriminant Analysis (LDA). Matching is performed by calculating Euclidean distances between the extracted feature vectors of reference and query biometric templates [18, 19].

4 Experimental Results and Discussion

4.1 Databases Used for Experimentation

The performance is evaluated on two different biometric modalities, i.e., face and palmprint. To study the functional performance of the proposed system on face modality, three different standard face databases– ORL, Extended Yale Face Data-

base B, and Indian face are used. ORL is an expression variant database consisting of 40 subjects with 10 images per subject capturing different facial expressions [20]. Extended YALE face database is an illumination variant database containing 64 near frontal images for 38 subjects under various illumination conditions [21]. Out of it only 10 images per subject having uniform illumination are selected. The Indian face database 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 [22]. For each database, 3 images are randomly selected for training database and 7 images for test database. CASIA and PolyU palmprint databases are used to study the functional performance of the proposed system on palmprint image templates. CASIA contains 5,239 palmprint images of left and right palms of 301 subjects thus a total 602 different palms [23]. PolyU database includes 600 images from 100 individuals, with 6 palmprint images from each subject [24]. For palmprint databases, per subject 2 images for training and 4 images for testing purposes are randomly selected after extracting the region of interest [25].

4.2 Performance Evaluation on Face and Palmprint Image Templates

The performance is determined using Equal Error Rates (EER) 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. The value is either positive or negative, according to the score assigned to that pattern. Higher values of *DI* indicate better decidability while classifying genuine and imposter populations. *DI* is calculated as

$$DI = \frac{|\mu_G - \mu_I|}{\sqrt{(\sigma_G^2 + \sigma_I^2)/2}} \tag{10}$$

Matching performance of the proposed approach is evaluated in case of stolen token scenario [18, 19]. It represents the worst case scenario when an attacker is always in possession of users' specific data or tokens. The stolen token scenario is simulated by assigning same random matrix R to each subject in the database. Matching is performed on transformed templates which are generated using same R for each subject in every database. It is expected that the system performance must not regress when it operates on transformed templates under stolen token scenario. Matching performance is also evaluated on the original (untransformed) templates using LDA which is used for comparison. Table 1 provides results for matching performance on conventional untransformed biometric templates and transformed templates using proposed approach under stolen token scenario for various databases. The ROC curves are shown in Fig. 2.

Table 1 Matching performance for face and palmprint templates

Modality	Database	Original		Proposed	
		EER (%)	DI	EER (%)	DI
Face	ORL	5.42	3.133	6.90	3.438
	Indian Face	11.11	2.398	11.53	2.352
	YALE	10.52	2.612	8.91	2.921
Palmprint	PolyU	0.62	7.569	0.56	8.735
	CASIA	2.34	5.083	2.50	4.183

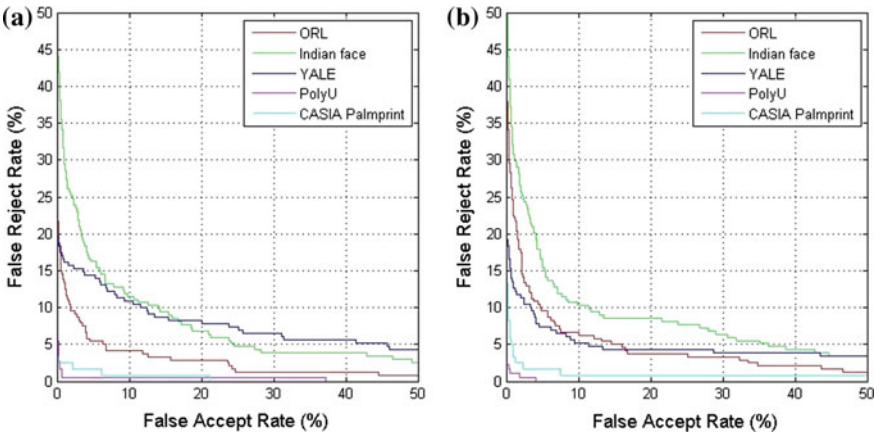

Fig. 2 ROC curves for matching performance **a** original domain **b** transformed domain

It can be observed that the matching performance, i.e., EER of proposed approach under stolen token scenario is comparable to non-cancelable based technique. The experimental results validate that the proposed approach transforms biometric templates while effectively preserving their discriminability and meets the performance evaluation criteria of cancelability under stolen token scenario. The genuine and imposter populations in transformed domain is well distributed. DI values obtained from genuine and imposter mean and variance in stolen token scenario are sufficiently high which indicate good separability among transformed templates. The performance in case of legitimate key scenario, when each subject is assigned different random matrix R results in nearly 0 % EER for all modalities and databases.

4.3 Invertibility Analysis

Consider the scenario, when the transformed template I^T and projection matrix R are available simultaneously. The inverse operation (decryption) requires the projection

of I^T over the inverse of random matrix R^{-1} as

$$I^{inv\_proj} = H_n \times ((H_n \times I^T \times H_n) \times R^{-1}) \times H_n \tag{11}$$

The next step requires an attacker to have the exact values over which modulus is computed for each row, i.e., the mean vector M, which is discarded immediately after transformation. Hence, it cannot be inverted. Yet, we consider a scenario where the exact vector M is approximated by the attacker using intrusion or hill climbing attacks. Then the inverse template should be computed as

$$I^{rec}(i,:) = I^{inv\_proj}(i,:) mod M(i) \tag{12}$$

To decrypt the information, inverse or psuedo-inverse of matrix R needs to be computed. However, for lossless recovery from encrypted data, the matrix R should be selected such that the elements of inverse matrix R^{-1} posses non-negative integral values. In our case the key space is restricted to random Achlioptas matrices comprising of +1, 0, or –1. It is possible to compute inverse or psuedo-inverse of these matrices but the inverted matrices are always found to possess non-integral and negative values. It makes the recovery of information very noisy on decryption and does not reveal original template.

4.4 Distinctiveness Analysis

To evaluate distinctiveness, ten different transformed templates corresponding to the same biometric are generated for each database by changing user-specific parameter (random projection matrix R). Mutual information content between each pair of transformed templates, C_r, is calculated using Eq. 13.

$$C_r(I_1, I_2) = \frac{\sum\sum(I_1 - \bar{I}_1)(I_2 - \bar{I}_2)}{\sqrt{(I_1 - \bar{I}_1)^2 + (I_2 - \bar{I}_2)^2}} \tag{13}$$

where $\bar{I}_1$,$\bar{I}_2$ represents the mean of templates I_1, I_2, respectively. The correlation index (CI) is the mean of all collected C_r values. Table 2 provides CI values between transformed templates for different modalities and databases. For example, average value of $I = 0.121$ means that two templates generated from the same biometric sample using different random matrices share 12.1 % of mutual information and are different to each other by 87.9 %. It is observed from Table 2 that CI values are low. This indicates that the proposed approach offers good revocability and diversity.

Table 2 Correlation index values for different databases

Modality	Face			Palmprint	
Database	ORL	Indian face	YALE	PolyU	CASIA
CI	0.121	0.132	0.112	0.095	0.134

5 Conclusion

The proposed approach successfully meets an important requirement of achieving good recognition rates in transformed domain and addresses stolen token scenario. Non-invertiblity being an important requirement is also ascertained without giving up on performance. The compaction of energy using HT before random projection allows mean vector M to coincide for templates belonging to same user. This way templates belonging to the same user are tend to have similar M. The ability to generate various transformed templates by changing the transformation parameter is evaluated in distinctiveness analysis which supports revocability and diversity.

References

1. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal **40** (2001) 614–634
2. Lacharme, P., Cherrier, E., Rosenberger, C.: Preimage attack on biohashing. In: International Conference on Security and Cryptography (SECRYPT). (2013)
3. Sutcu, Y., Sencar, H.T., Memon, N.: A secure biometric authentication scheme based on robust hashing. In: Proceedings of the 7th workshop on Multimedia and security, ACM (2005) 111–116
4. Teoh, A.B.J., Ngo, D.C.L.: Biophasor: Token supplemented cancellable biometrics. In: Control, Automation, Robotics and Vision, 2006. ICARCV'06. 9th International Conference on, IEEE (2006) 1–5
5. Teoh, A., Yuang, C.T.: Cancelable biometrics realization with multispace random projections. Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on **37** (2007) 1096–1106
6. Lumini, A., Nanni, L.: An improved biohashing for human authentication. Pattern recognition **40** (2007) 1057–1065
7. Ratha, N., Connell, J., Bolle, R.M., Chikkerur, S.: Cancelable biometrics: A case study in fingerprints. In: Pattern Recognition, 2006. ICPR 2006. 18th International Conference on. Volume 4., IEEE (2006) 370–373
8. Tulyakov, S., Farooq, F., Govindaraju, V.: Symmetric hash functions for fingerprint minutiae. In: Pattern Recognition and Image Analysis. Springer (2005) 30–38
9. Ang, R., Safavi-Naini, R., McAven, L.: Cancelable key-based fingerprint templates. In: Information Security and Privacy, Springer (2005) 242–252
10. Boult, T.E., Scheirer, W.J., Woodworth, R.: Revocable fingerprint biotokens: Accuracy and security analysis. In: Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on, IEEE (2007) 1–8
11. Farooq, F., Bolle, R.M., Jea, T.Y., Ratha, N.: Anonymous and revocable fingerprint recognition. In: Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on, IEEE (2007) 1–7

12. Dasgupta, S., Gupta, A.: An elementary proof of the johnson-lindenstrauss lemma. International Computer Science Institute, Technical Report (1999) 99–006
13. Matoušek, J.: On variants of the johnson–lindenstrauss lemma. Random Structures & Algorithms **33** (2008) 142–156
14. Indyk, P., Motwani, R.: Approximate nearest neighbors: towards removing the curse of dimensionality. In: Proceedings of the thirtieth annual ACM symposium on Theory of computing, ACM (1998) 604–613
15. Dasgupta, S.: Learning mixtures of gaussians. In: Foundations of Computer Science, 1999. 40th Annual Symposium on, IEEE (1999) 634–644
16. Achlioptas, D.: Database-friendly random projections. In: Proceedings of the twentieth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, ACM (2001) 274–281
17. Bingham, E., Mannila, H.: 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 (2001) 245–250
18. Bartlett, M.S., Movellan, J.R., Sejnowski, T.J.: Face recognition by independent component analysis. Neural Networks, IEEE Transactions on **13** (2002) 1450–1464
19. Connie, T., Teoh, A., Goh, M., Ngo, D.: Palmprint recognition with pca and ica. In: Proc. Image and Vision Computing, New Zealand. (2003)
20. ORL face database: (AT&T Laboratories Cambridge) http://www.cl.cam.ac.uk/.
21. Yale face database: (Center for computational Vision and Control at Yale University) http://cvc.yale.edu/projects/yalefaces/yalefa/.
22. The Indian face database: (IIT Kanpur) http://vis-www.cs.umas.edu/.
23. CASIA palmprint database: (Biometrics Ideal Test) http://biometrics.idealtest.org/downloadDB/.
24. PolyU palmprint database: (The Hong Kong Polytechnic University) http://www4.comp.polyu.edu.hk/biometrics/.
25. Kekre, H., Sarode, T., Vig, R.: An effectual method for extraction of roi of palmprints. In: Communication, Information & Computing Technology (ICCICT), 2012 International Conference on, IEEE (2012) 1–5