Indonesian Journal of Electrical Engineering and Computer Science
Vol. 7, No. 3, September 2017, pp. 877 ~ 886
DOI: 10.11591/ijeecs.v7.i3.pp877-886

Random Projection-based Cancelable Template Generation for Sparsely Distributed Biometric Patterns

P. Punithavathi[*1], S. Geetha[2]
School of Computing Science & Engineering, VIT University Chennai Campus, Chennai, Tamil Nadu, India
*Corresponding author, e-mail: p.punithavathi2015@vit.ac.in

Abstract

Cancelable biometrics, a template transformation approach, attempts to provide robustness for authentication services based on biometrics. Several biometric template protection techniques represent the biometric information in binary form as it provides benefits in matching and storage. In this context, it becomes clear that often such transformed binary representations can be easily compromised and breached. In this paper, we propose an efficient non-invertible template transformation approach using random projection technique and Discrete Fourier transformation to shield the binary biometric representations. The cancelable fingerprint templates designed by the proposed technique meets the requirements of revocability, diversity, non-invertibility and performance. The matching performance of the cancelable fingerprint templates generated using proposed technique, have improved when compared with the state-of-art methods.

Keywords: *Cancelable fingerprint template, Discrete fourier transformation, Random projection, Random matrix, Template transformation*

1. Introduction

1.1. Biometrics

Biometrics refers to the measurable physiological (face, fingerprints, hand geometry, iris, ear, palm prints, etc.,) and behavioral (gait, speech, signature, key stroke, etc.,) characteristics of an individual. The biometrics has been largely employed in sensitive applications to authenticate users, instead of passwords or tokens. The biometric system is comprised of; 1) a sensor unit to image raw biometrics, 2) a feature extraction unit to generate feature vector from biometric image, 3) a database to store feature vector in template format, 4) a matching unit to match user's template with stored template, 5) a decision unit to decide access grant.

1.2. Attacks on Biometric System

Different levels of attacks were identified by Patel et al. in [1], which can be launched against biometric system. These attacks on the biometric system are shown in Figure 1.

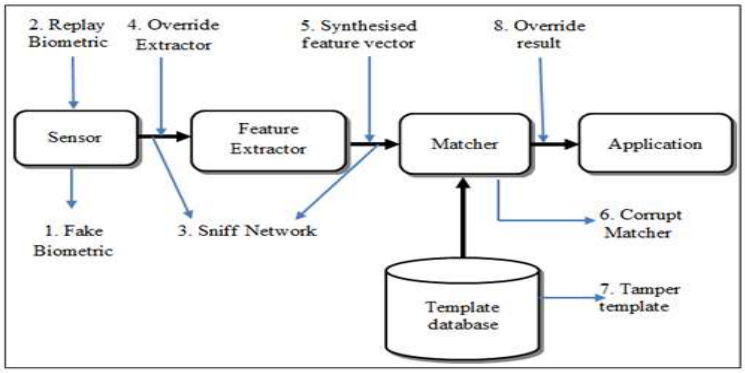


Figure1. Attacks on Biometric System

Received May 12, 2017; Revised July 30, 2017; Accepted August 14, 2017

a) fake biometric trait such as an artificial finger may possibly be presented at the sensor
b) illegally captured data may be resubmitted to the system
c) feature extracting module may be replaced by illegal Trojan horse program to produce pre-determined feature sets
d) genuine feature sets may be replaced with fake feature sets
e) matcher may be replaced by illegal programs like Trojan horse which will always output high scores thereby challenging system security
f) stored templates may be modified or removed, or new templates may be introduced into the database
g) data within the communication channel between various modules of the system may be modified, and the final decision of the matcher may be overwritten

Various methods such as steganography, watermarking, biometric cryptosystems and chaotic encryption schemes, to overcome these attacks can be found respectively in [2]-[5]. Though these methods are robust against several attacks, they lack diversity and prevent each and every user to be registered to number of applications with single biometric template alone. Cancelable biometrics is a solution to provide diversity so that users can enrol to numerous applications using corresponding transformed template.

1.3. Cancelable Biometrics

Cancelable biometrics (pioneered by Soutar et al. in 1998 [6], but furnished by Bolle et al. in 2002 [7]) is a template transformation approach to secure the biometric template. These non-invertible transformations are applied to the biometric input either at signal-level or feature-level. The matching is performed in the transformed domain. By changing the transformation factor, number of transformed templates can be acquired, correspondingly from single biometric template. These transformed templates can be canceled and revoked easily like password, in the case of biometric compromise. A transformed template must agree the following properties:

a) Diversity – Multiple transformed templates should be generated corresponding to the enrolment of users into multiple applications using same biometrics.
b) Non-invertibility – The transformed templates once generated should not be inversed at any point.
c) Revocable – New transformed templates must be generated to replace the compromised template in the database.
d) Performance – The matching performance of the templates in transformed domain should not degrade even across multiple applications, when compared to conventional biometric template matching schemes.

2. Literature Survey

Ratha et al [8] proposed a case study of cancelable biometrics applied to fingerprint using Cartesian, radial and functional transformations. Jin et al [9] proposed biohashing which generates Biocodes based on the projection of an orthonormal random matrix (generated by a pseudo random generator), on biometric features. Boult et al [10] proposed revocable fingerprint generating system in which biometric feature is segmented into two parts. The first part is encrypted and the second part is left to support approximate matching. Teoh and Yaung [11] proposed multispace random projection in which a fixed-length vector acquired from raw biometric features, are projected on a sequence of random sub-spaces derived from user-specific pseudorandom number. Kaur and Khanna [12] proposed random projection for generating cancelable templates of palmprint and face.

The non-invertible transformations mostly yield transformed templates in binary form, out of the binary biometric template. The fact is that the binary representations can be easily managed and stored. Moreover the binary representations offer simplicity in terms of matching. But the binary representation of transformed template is highly susceptible to inversion in case if the binary biometric template is sparsely distributed. Hence there is a strong requirement of a template transformation technique that secures even sparsely distributed binary biometric representations.

The cancelable templates designed by using the proposed transformation technique meets the requirements of diversity, revocability, non-invertibility and matching performance,

evaluated over the publicly available databases DB1 and DB2 of FVC2002 [13] and FVC2004 [14]. The contributions of the proposed technique are summarized as follows:

a) Using Discrete Fourier Transform (DFT) spreads the spectrum of sparsely distributed binary biometric representations
b) The proposed random projection technique is effective in securing the binary biometric templates while preserving the pair-wise distance between them even after transformation
c) Moreover the computational complexity of the proposed technique is very less which makes it suitable for use in mobile phones
d) The recognition performance of the proposed technique has been comparatively analysed and shows improvement with respect to the Equal Error Rate (EER) of the existing methods.

The paper is organised as follows: Section 3 gives an introduction to the basics of DFT and random projection technique. Section 4 describes the proposed technique for extracting cancelable fingerprint template. Section 5 provides an insight to the comprehensive analysis of the results. Section 6 gives conclusion and future work.

3. Introduction to DFT and Random Projection

3.1 DFT

Let us assume that a binary fingerprint template (v_b) shown in equation (1), denote the binary biometric representation extracted from the biometrics, before transformation.

$$v_b = [b(0)b(1),\ldots,b(m-1)]^X \quad (1)$$

where $b(i) \in \{0,1\}$; and i ranges from 0 to $(m-1)$, m representing the size of the template. It is clear that v_b has to be secured because it contains vital information regarding the biometrics of user. Since it is in binary form, the transformation operations on v_b can narrow down the search space (during attempts to invert the cancelable template); especially when elements of v_b are non-uniformly and sparsely distributed. Hence DFT can be applied to v_b prior to the application of random projection, in-order to achieve dense data representation.
We now take N-point DFT of v_b as shown in (2).

$$v_B = Fv_b \quad (2)$$

where F is a DFT matrix as shown in (3), and $N = 2^n$ and $N \geq m$. The value of v_B can be represented as shown in (4).

$$F = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & W & W^2 & \cdots & W^{(N-1)} \\ 1 & W^2 & W^4 & \cdots & W^{2(N-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & W^{(N-1)} & W^{2(N-1)} & \cdots & W^{(N-1)(N-1)} \end{bmatrix} \quad (3)$$

$$v_B = [B(0)B(1),\ldots,B(m-1)]^X \quad (4)$$

where $W = e^{-j2\pi/N}$. The DFT matrix is a unitary matrix and the DFT operation is highly invertible. It is to be noted that purpose of taking DFT is just to scatter the sparsely distributed values of v_b .

3.2 Random Projection Technique

The Johnson-Lindenstrauss (JL) Lemma [15] and [16] basically states that a set of points P in a higher-dimensional Euclidean space $\Re^N$ can be embedded into a lower-dimensional Euclidean space $\Re^n$ such that the pair-wise distance of any two points is maintained approximately. The JL lemma is given as:

Let $\varepsilon \in (0,1)$ be given. For every set P of #(P) points in $\Re^N$, if *n* is a positive integer such that,

$$n > n0 = o(\frac{ln(\#(P))}{\varepsilon^2}) \quad (5)$$

Then it can be concluded from equation (5), that there exists a Lipschitz mapping $f : \Re^N \to \Re^n$ such that

$$(1-\varepsilon)\|x-y\|^2 \le \|f(x)-f(y)\|^2 \le (1+\varepsilon)\|x-y\|^2 \quad (6)$$

for all $x, y \in P$.

The function *f* is a linear mapping represented by *k*×*d* matrix Ψ which has its components drawn randomly from specific probability distributions. Hence it is clear that the statistical characteristics required for recognition can be preserved even while changing the original form of the data. The matrices which satisfy (6) for any given set of points P are as follows (provided n satisfies the condition of JL lemma):

a) The entries $\psi_{i,j}$ of Ψ are realizations of independent Gaussian random variables
b) The entries $\psi_{i,j}$ of Ψ are realizations of ±1 Bernoulli random variables with a probability of 0.5
c) The entries $\psi_{i,j}$ of Ψ are realizations of related distributions including values of ±√3 (each with a probability of 0.167) and 0 (with a probability of 0.67)

All the three matrices have proved to provide successful projection matrices which end up in similar results. But we have used Gaussian projections in our experiments. The process of projecting the binary biometric representation v_B on random matrix Ψ is defined as:

$$T_{B(d\times N)} = \psi(d\times k)\, v_{B(k\times N)} \quad (7)$$

The pair-wise distances between the vectors must be preserved before and after transformation. The extent of preservation of pair-wise distances between the vectors highly depends upon the projection vectors $\omega_i \in \Psi$. According to *JL* lemma, the critical property of the random projection matrix is that its column vectors ω_i must be orthogonal to each other. This can be achieved by using Gram Schmidt orthogonalization technique. But this technique increases the computational complexity to a great magnitude.

Several measures have been proposed to reduce the computational complexity. In [17], it has been reported that the condition of orthogonality must be eliminated while using random projections to approximate nearest-neighbour in Euclidean space of higher dimension. As an extension to proof, they used a random projection matrix whose column entries are independent random variables with Gaussian distribution. The projection of such a matrix has possesses chi-square distribution with *k*-degrees of freedom. Further the 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 $(1 \pm \sigma, where\ 0 < \sigma < 1)$. Hence it is clear that a random projection matrix whose elements are normally distributed preserve the pair-wise distance between vectors even after transformation. This reduces the computational complexity of generating random matrix since the orthogonality condition is dropped.

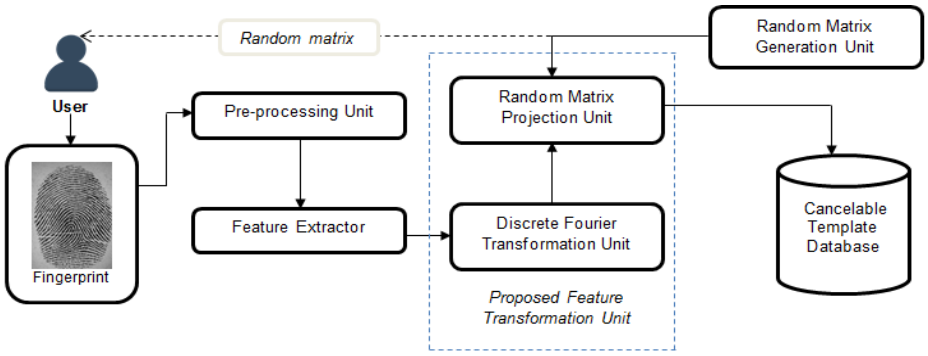
4. Proposed System For Generation Of Complex Cancelable Fingerprint Template

4.1 Generation of Binary Fingerprint Template

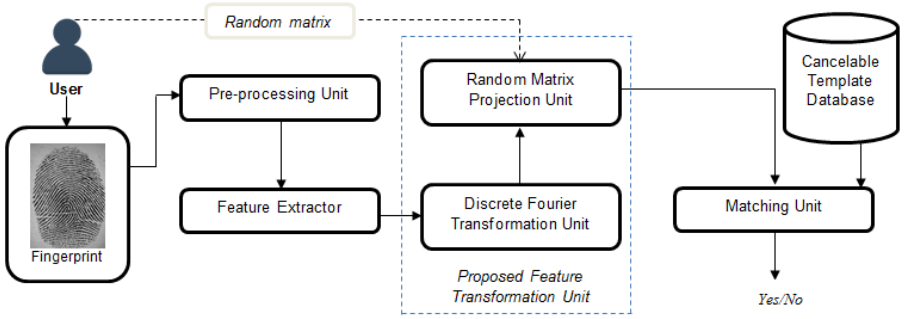
The input fingerprint image from sensor is pre-processed using enhancement and binarization techniques. Then the binarized image is subjected to thinning process so that the ridges become one pixel wide. The ridges are thin curved lines in fingerprint, which may bifurcate or terminate. These bifurcations and terminations are called minutia. Each and every fingerprint has about 70-150 minutia points. Each i^{th} minutia is represented by $M_i = [x_i, y_i, t_i, \theta_i]$. Here, x_i and y_i, θ_i ranging from $[0, 2\pi]$, and θ_i represent the position, the orientation, and the type of minutiae (bifurcation or termination), respectively. The binary fingerprint template (v_b) is generated using these minutia points as shown in [18].

4.2 System Model Using Proposed Technique

The system model of the proposed cancelable biometric scheme (shown in Figure 2) involves two processes namely – enrolment and verification.



(a) Enrolment Phase



(b) Verification Phase

Figure 2. Block Diagram of Proposed Technique

The enrolment process involves generation of cancelable fingerprint template from binary fingerprint template using the proposed transformation technique. This can be modelled mathematically with respect to the proposed system (using the equations (2), (4) and (7)) as follows:

$$T_B = \psi_F v_b \tag{8}$$

To summarize the process, the binary fingerprint template is subjected to DFT and then random projection to generate a cancelable fingerprint template. The verification process (performed in transformed domain) involves transformation of query binary fingerprint template (say v_q) into

query cancelable fingerprint template (say T_q) using the equation (8). The verification process also involves making a binary matching decision after calculating the distance D between T_B and T_q ($D(T_B, T_q)$) such that:

$$D(T_B, T_q) = \frac{d(T_B, T_q)}{(w(T_B) + w(T_q))} \quad (9)$$

$$V = \begin{cases} 1, D(T_B, T_q) < T \\ 0, otherwise \end{cases} \quad (10)$$

where T is a predefined threshold. The value of $D(T_B, T_q)$ is given by Equation (9). The templates T_B and T_q are said to be matching only if $V = 1$, as represented by Equation (10). For convenience, the binary fingerprint template, DFT matrix and random matrix are all chosen to be of same dimension.

4.3 Steps Involved In Proposed Technique

The input to the proposed system is the features extracted from the user's fingerprint. The steps involved in enrolment phase and verification phase have been listed below.

Steps involved in enrolment phase:

Input: Features of fingerprint v_b

Output: cancelable fingerprint template T_B, and random matrix Ψ

Step 1: DFT unit generates N-point DFT of v_b by using equation (2) and outputs v_B
Step 2: Random matrix generation unit generates Ψ
Step 3: The feature transformation unit acts as random project unit which projects Ψ on v_B, and generates a T_B
Step 4: T_B is stored in the database
Step 5: The random matrix Ψ is given to the user for usage in verification phase

Steps involved in verification phase:

Input: Features of fingerprint v_b and random matrix Ψ

Output: Decision Yes or no based on matching probability of T_B and T_q

Step 1: DFT unit generates N-point DFT of v_b by using equation (2) and outputs v_B
Step 2: The feature transformation unit projects Ψ (input by user) on v_B, and generates a query template say T_q
Step 3: The matching unit matches T_B and T_q as in equation (10), and outputs yes or no decision based on the matching probability

5. Results and Discussions

5.1 Image Dataset

The proposed system for generating cancelable fingerprint template has been tested on publicly available datasets in DB1 and DB2 of FVC2002 and FVC 2004. The details of the datasets have been given in Table 1. The experiment has been carried out using MATLAB R2015a. Both genuine and imposter tests have been conducted on the four databases. The first image of each finger from the databases has been used as template. The second image of each finger from the databases has been used as query images. This has accounted to 100 genuine scores and $((100 \times 99)/2) = 4950$ imposter scores for each database.

Table 1. Details of the datasets used in experimentation

Details	FVC2002 DB1	FVC2002 DB2	FVC2004 DB1	FVC2004 DB2
No. of fingers	100	100	100	100
No. of images of each finger	8	8	8	8
Size of image	388×374	296×560	640×480	328×364
Image format	Tagged Image File Format	Tagged Image File Format	Tagged Image File Format	Tagged Image File Format

5.2 Complexity Analysis

The usage of DFT and random projection in the proposed approach leads to reduced computational complexity. Let $O(\cdot)$ denote the computational complexity of an algorithm. The proposed technique is comprised of N-point DFT and random projection. The N-point DFT can be implemented using Radix-2FFT algorithm [19]. The computational complexity of Radix-2FFT algorithm is estimated to be $O(N\log_2 N)$. The computational complexity of random projection is $O(kdN)$. The overall computational complexity is calculated to be $O[N(\log_2 N + kd)]$. This low computational complexity makes the proposed technique to be suitable for memory and power constrained devices like mobile phones.

5.3 Matching-Performance Analysis

The performance is evaluated using Equal Error Rates (EER). The EER calculated with respect to False Rejection Rate (FRR) and False Acceptance Rate (FAR), has been used to examine the matching performance of the original as well as the transformed templates. The Equations (11) and (12) are used in the calculation of FRR and FAR, respectively.

$$FRR = (Number\ of\ failed\ rejections)/(Number\ of\ legitimate\ access\ attempts) \times 100 \quad (11)$$

$$FAR = (Number\ of\ false\ acceptances)/(Number\ of\ imposter\ attempts) \times 100 \quad (12)$$

$$GAR = 1 - FRR \quad (13)$$

For each dataset, FRR is measured by matching a selected query cancelable fingerprint template with the same template stored templates. FAR is measured by matching a selected query cancelable fingerprint template with all the templates in the gallery. EER can be defined as the error trade-off between FAR and FRR i.e., FRR=FAR at particular threshold value.

The performance of a system is always inversely proportional to the value of EER. The EER of cancelable fingerprint template is found to be better than the EER of the transformed templates in [20, 21]. In [20], a randomized graph-based Hamming embedding technique has been proposed to generate transformed fingerprint template in binary format. In [21] a blind system identification approach has been proposed to generate transformed fingerprint template in complex-vector form. Comparative results are shown in Table 2.

Table 2. EER (%) Comparison

Methods	FVC2002 DB1	FVC2002 DB2	FVC2004 DB1	FVC2004 DB2
(Jin, Lim, Teoh, and Goi, 2014) [20]	4.36	1.77	-	21.82
(Wang, and Hu, 2016) [21]	3	2	-	-
Proposed System	1.27	2.56	8.75	13.39

5.4 Non-Invertibility Analysis

Non-invertibility is an important characteristic of cancelable biometric system by ensuring that the transformation applied is always one sided. It should not be reversible. In other words, the transformed template T_B should not yield any information about the original binary biometric representation v_b. Let us consider a stolen-token scenario where both T_B and the random matrix Ψ are acquired by an adversary. Now the adversary may learn the

transformation process and try to acquire the raw biometric features v_b out of the possessed evidences. But since the proposed system is an underdetermined system as proposed in [22], there may be infinite number of solutions to v_b. The chance of guessing the correct original binary biometric representation is minimal.

The Receiver Operating Characteristic (ROC) for each dataset in stolen-token scenario is plotted in Figure 3(a)-3(d). The ROC of the binary biometric representation (pre-transformation) is compared with that of the cancelable fingerprint template (post-transformation). It is clear that the recognition performance of the templates before and after transformation is very similar for FVC2002 DB1 and DB2. But it is highly dissimilar in case of FVC20024 DB1 and DB2. This is due to poor quality of the images of in FVC20024 DB1 and DB2.

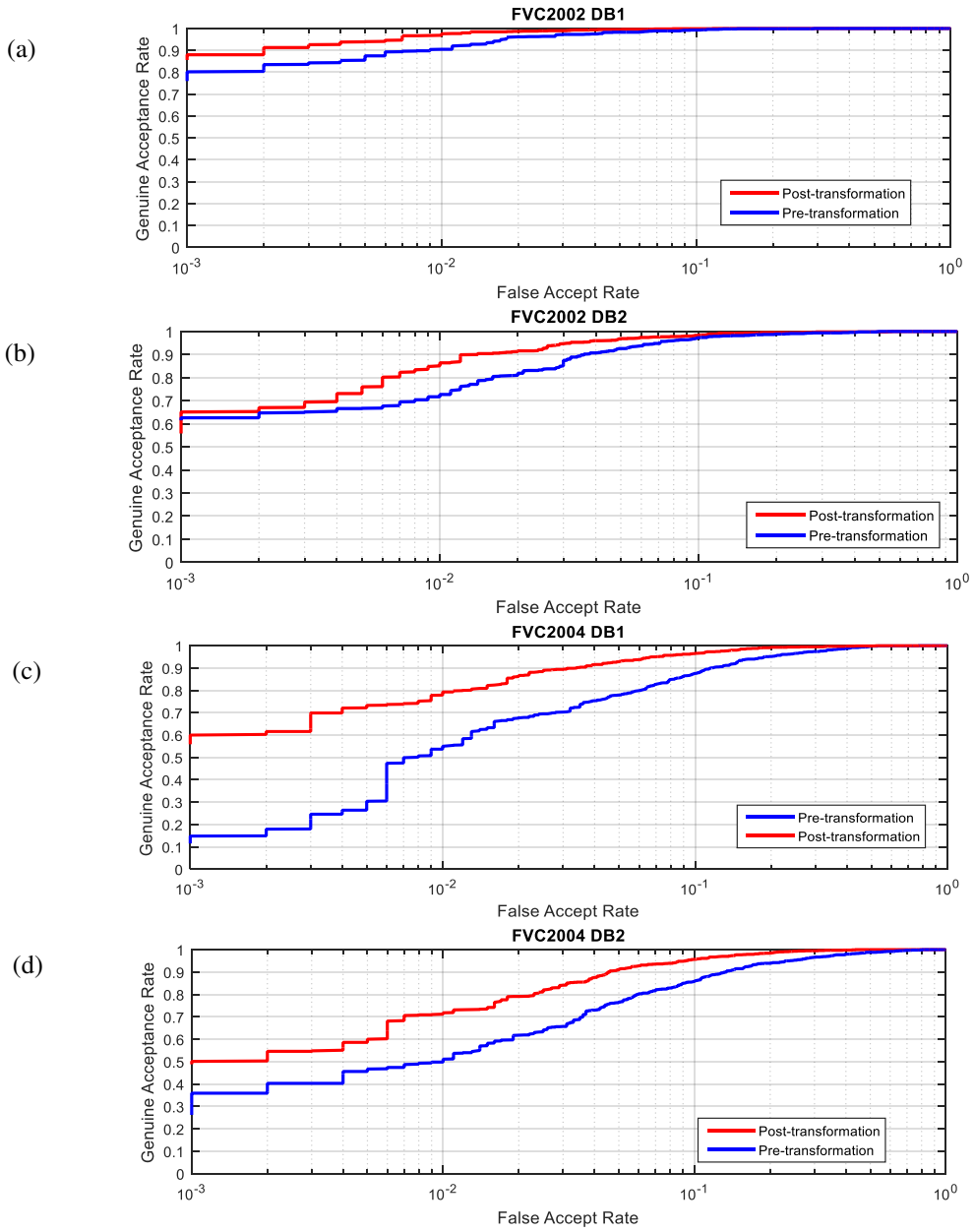


Figure 3. ROC Curves (a) FVC2002 DB1; (b) FVC2002 DB2; (c) FVC2004 DB1; (d) FVC2004 DB2

5.5 Diversity Analysis

Different cancelable templates (say T1 and T2) have been generated for each database by using corresponding random matrices. Then correlation (C) is calculated between each pair of cancelable template using Equation (14). Let correlation index (C') be the mean of all values of C corresponding to the cancelable templates generated for respective fingerprint. Table 3 shows the value of C' of cancelable templates for different FVC databases. If the value of C' = 0.0022, then two templates generated from same biometric sample using different random matrices share 0.22 % of mutual information.

$$C(T1,T2)=\frac{\sum\sum(T1-\overline{T1})(T2-\overline{T2})}{\sqrt{(T1-\overline{T1})^2+(T2-\overline{T2})^2}} \quad (14)$$

Table 3. Correlation Coefficients of Templates

Database	*C'*
FVC2002 DB1	0.0022
FVC2002 DB2	0.0024
FVC2004 DB1	0.0019
FVC2004 DB2	0.0023

6. Conclusion

We have proposed a random projection-based approach for designing cancelable fingerprint templates containing complex biometric representations. The feature templates of a fingerprint may be sparse. The proposed technique is robust even in such situations because the DFT spreads the spectrum and reduces the sparsity greatly. The cancelable fingerprint templates generated using the proposed approach, satisfy the basic properties of cancelable biometrics-revocability, diversity, non-invertibility and matching performance. By using random projection-based approach for transformation of binary biometric features, it becomes computationally efficient; and highly suitable for resource-limited applications, e.g., mobile phones. The effectiveness of the proposed technique can be tested on different modalities in future.

Acknowledgements

Authors are thankful to the Management of VIT University-Chennai Campus. The first author has been supported by Visvesvaraya PhD Scheme funded by Media Lab Asia, DeitY, Government of India.

References

[1] Patel VM, Ratha NK, Chellappa R. Cancelable biometrics: A review. IEEE Signal Processing Magazine. 2015 Sep;32(5):54-65.

[2] Balasubramanian C, Selvakumar S, Geetha S. High payload image steganography with reduced distortion using octonary pixel pairing scheme. Multimedia tools and applications. 2014 Dec 1;73(3):2223-45.

[3] Thanki R, Borisagar K. Security of Biometric Data Using Compressed Watermarking Technique. International Journal of Electrical and Computer Engineering. 2014 Oct 1;4(5):758.

[4] Jin Z, Teoh AB, Goi BM, Tay YH. Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. Pattern Recognition. 2016 Aug 31;56:50-62.

[5] Abundiz-Pérez F, Cruz-Hernández C, Murillo-Escobar MA, López-Gutiérrez RM, Arellano-Delgado A. A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler Map. Mathematical Problems in Engineering. 2016 Jul 31;2016.

[6] Stojanov R, Gilroy Soutar G, Roberge D, Kumar V. Biometric encryption using image processing. SPIE, Optical Security and Counterfeit Deterrence Techniques H. 1998;3314:178-88.

[7] Bolle RM, Connell JH, Ratha NK. Biometric perils and patches. Pattern Recognition. 2002 Dec 31;35(12):2727-38.

[8] Ratha N, Connell J, Bolle RM, Chikkerur S. Cancelable biometrics: A case study in fingerprints. InPattern Recognition, 2006. ICPR 2006. 18th International Conference on 2006 Aug 20 (Vol. 4, pp. 370-373). IEEE.

[9] Jin AT, Ling DN, Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition. 2004 Nov 30;37(11):2245-55.

[10] Boult TE, Scheirer WJ, Woodworth R. Revocable fingerprint biotokens: Accuracy and security analysis. InComputer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on 2007 Jun 17 (pp. 1-8). IEEE.

[11] Teoh AB, Yuang CT. Cancelable biometrics realization with multispace random projections. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics). 2007 Oct;37(5):1096-106.

[12] Kaur H, Khanna P. Gaussian random projection based non-invertible cancelable biometric templates. Procedia Computer Science. 2015 Jan 1;54:661-70.

[13] "FingerprintVerification Competition," 2002. [Online]. Available: http://bias.csr.unibo.it/fvc2002/.

[14] "FingerprintVerification Competition," 2004. [Online]. Available: http://bias.csr.unibo.it/fvc2004/.

[15] Johnson WB, Lindenstrauss J. Extensions of Lipschitz mappings into a Hilbert space. Contemporary mathematics. 1984 May;26(189-206):1.

[16] Bingham E, Mannila H. Random projection in dimensionality reduction: applications to image and text data. InProceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining 2001 Aug 26 (pp. 245-250). ACM.

[17] Har-Peled S, Indyk P, Motwani R. Approximate Nearest Neighbor: Towards Removing the Curse of Dimensionality. Theory of computing. 2012 Jan 12;8(1):321-50.

[18] Wang S, Hu J. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recognition. 2014 Mar 31;47(3):1321-9.

[19] Proakis JG, Manolakis DG. Digital Signal Processing: Principles, Algotithms, and Applications, Prentice Hall, 1996.

[20] Jin Z, Lim MH, Teoh AB, Goi BM. A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. Pattern Recognition Letters. 2014 Jun 1;42:137-47.

[21] Wang S, Hu J. A blind system identifaication approach to cancelable fingerprint templates. Pattern Recognition. 2016 Jun 30;54:14-22.

[22] Wang S, Hu J. Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach. Pattern Recognition. 2012 Dec 31;45(12):4129-37.