Literature Review on Cancellable Biometrics Face

YEAR 2007

Gurpreet Singh
079154192
School of Electrical Electronics and Computer Engineering

ACKNOWLEDGEMENT

I extend my sincere thanks to Professor S. S. DLAY for his guidance and continuous support.

CONTENTS

LIST OF FIGURES

ACRONYMS

1. FRR : FALSE REJECTION RATIO
2. FAR : FALSE ACCEPTANCE RATIO
3. WFMT : WAVELET FOURIER–MELLIN TRANSFORM FRAMEWORK
4. RMQ : RANDOM MULTISPACE QUANTISATION
5. MACE : MINIMUM AVERAGE CORRELATION ENERGY
6. PSR : PEAK TO SIDE LOBE RATIO
7. STD : STANDARD DEVIATION
8. ACE : AVERAGE COORELATION ENERGY
9. PCA : PRINCIPLE COMPONENT ANALYSIS
10. ICA : INDEPENDENT COMPONENT ANALYSIS
11. TRN: TOKENISED RANDOM NUMBER

Abstract

Although, biometrics provide high confidence and trusted security, despite of its advantages it has disadvantages in the area of privacy. In order to remove this problem cancellable biometrics concept was introduced. This review gives the introduction to the subject. It treats with the approach that it contains intentional, repeatable distortion of a biometric signal based on a chosen transform. With this approach original biometrics cannot be recovered. This review gives the explanation to terms like Biohashing, Biophasors, Random Multispace Quantization This review shows how much the recognition accuracy or performance is gained. Cancellable biometrics offers two outcomes known as False Accept Rate (FAR) and false Reject Rate (FRR). And cancellable biometrics aims to get zero FAR and FRR.

1. INTRODUCTION

A biometric authentication system is a system that depends on the physical feature of the human body for identification. This is shown by [1] that biometric authentic system consists of various modules or stages as shown in figure:

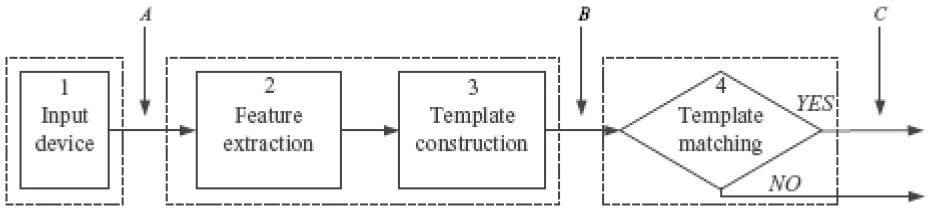


FIGURE (1). Biometric Authentication System **[1]**

It is system that is challenging the problems in traditional systems like PIN and Token Systems. Biometric is defined as a unique physical characteristic of the human body t hat can be used to verify the identity [2].
The names of few which are unique and universal for a good performance application such as face, iris, fingerprint, retina. But mostly used is biometric face recognition[3], although other biometric authentication and face recognition have merged with recent developments and improvements, there still exists a security problem i.e. the biometric information is not secure. This drawback of not protecting biometric information is overcome by cancellable biometrics, which protects the biometric data by transforming the data into non linear transform (domain) where data can't be inverse transformed to its original form.

The biggest problem with biometrics is the unreliability of individual bits in the used template. Biometrics measurements are being made of attributes of the human body are distorted or noisy by nature, while cryptography demands correctness in keys to be used. There has been made large attempts to bridge the gap between the fuzziness of biometrics from key stroke patterns and facial characteristics [4].

The concept of cancellable biometrics was proposed by [5]. The main behind this is to enhance security by transforming the original data to a certain biometric domain, where recognition can be accurately performed. And can not be retransformed to its original form. [6] Introduced an approach that uses tokenised pseudo random number and Wavelet Fourier Transform Mellin Transform Framework(WFMT). The method contains two components generation of invariant and discriminative face feature with a moderate degree of offset using the WFMT, to attain the facehash by a serial number goes through a discretisation process. This number is obtained by the product operation between face features and random numbers. D. Maltoni [7], the objective so such a cancellable biometrics template is given as:

1) Diversity: this means that the same cancellable template cannot be used in two different applications.

2) Reusability: this uses straightforward recalling and reuse in the compromise event.

3) Cancellable biometrics has a non inveretibility of template compilation to prevent the data from being recovered.

4) Performance: recognition performance should not be deteriorated.

This is shown by Goh et al. [4] and Teoh et al. [8] and [9] introduced biometric hashing framework i.e. inner product biometric vectors and token derived random sequences. Biohashing is the one way transformation equivalent cryptographic cipher [10], there by providing a great degree of protection to the biometric data. This process comprises of three stages:

1) feature extraction
2) random multispace mapping
3) quantisation

1.1 PERFORMANCE OF BIOMETRIC SYSTEMS

In the cancellable biometric authentication system, by setting the operating points i.e threshold, the false accept rate and false reject rate can be set. This is not possible to get both (FAR and FRR) low or close to at the same time. The FAR can get close to zero by setting the high threshold and similarly on the contrary at low threshold the value of FFR can be close to zero. Cancellable biometrics systems operate at a low FAR to provide high security [3] and [1].

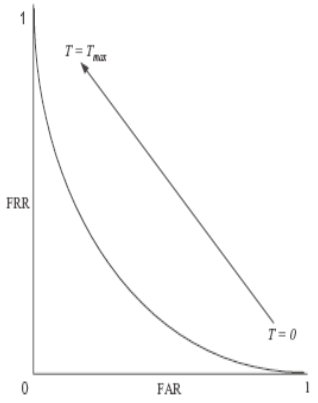


FIGURE (2). A roc curve is the relation between the FFR and FAR As a function of decision threshold T, **[3]** and **[1]**

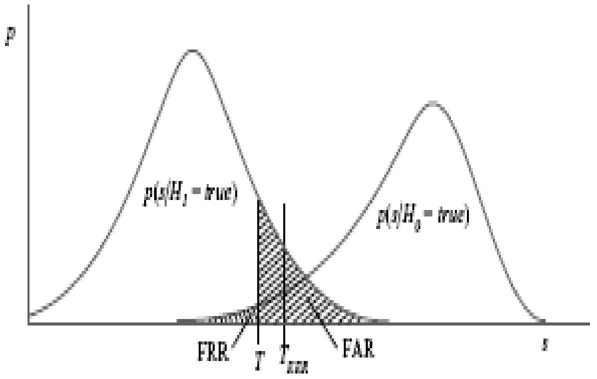


FIGURE (3).two types of error rates in biometric authentication system, **[3]** and **[1]**

1.2 AIMS

- exploring ways to stop invasion of privacy i.e. measures to enhance security of biometric data.
- Predicting the ways to get 100 percent accuracy (performance) in biometric system.
- Defining the algorithms which can't be inverted i.e. biometric data can not be transformed to its original form.

1.3 OBJECTIVE

- Investigate different types of biometrics algorithms which are practical enough to give the accurate end results.
- Explore ways to find solution to the wide spreading security related problems.
- Innovate new ideas to make further advancements in the cancellable face recognition technique.

LITERATURE REVIEW

2. CANCELLABLE BIOMETRICS

Cancellable biometrics concept was proposed by [5]. Several methods for generating cancellable biometrics have been proposed like Morphing, Biophasers, Biohashing and Random Multispace Quantisation. The basic idea behind Cancellable Biometrics is to transform to a original biometric data into a different domain, from where then the recognition can be done perfectly, and cannot be invertible into its original form. This method uses a tokenised pseudo random number and wavelet Fourier–Mellin transform framework (WFMT) for face recognition. The method comprises two components one is, generation of invariant and discriminative face feature with moderate degree of offset using W FMT, and to attain the facehash by a serial number goes through a discretisation process. The number is obtained from the product of the face features and random numbers. This is shown by M.Savvides [11], the cancellable biometrics is obtained by encrypting a set of training images to construct a minimum average correlation energy filter(MACE) for face authentication. The filter is then convolved with the original to produce the template. By changing the convolution kernels of the filters he biometric templates can be reproduced from the original biometric. Thus cancellable biometrics can be defined as the intentional, unique repeatable distortion of a biometrics signal based on certain chosen transform or domains [5][1].

2.1 MORPHING TECHNIQUE

A Morphed image is enrolled for face recognition. Morphing is the regular pattern or grid that is overlaid on the image after transforming the face image into canonical form as shown by [5].

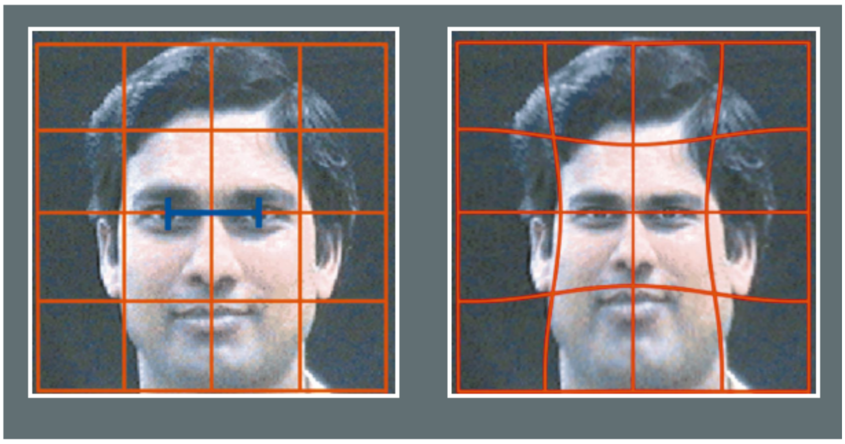


FIGURE (4). Distortion transform based on image morphing , **[5]**

In the Morphing method distortion transforms can be done in signal domain or it can also apply feature domain. The biometric signal can be processed as usual and then the extracted features can be reshaped. The bit strength of the system can be increased via a suitable transform by extending a template to a large representation space. It is important that the transform should not be transferrable to its original biometric form so to keep privacy of the biometric information.

Grid morphing and block representation are the examples of the transforms at signal level. Original image is shown with an overlaid grid levelled with the g=feature of the face is shown in figure (4). The next image shows the resulting distortion of the face. This is shown by [5] that a block structure is composed on the image levelled with characteristics points as shown in figure (5).

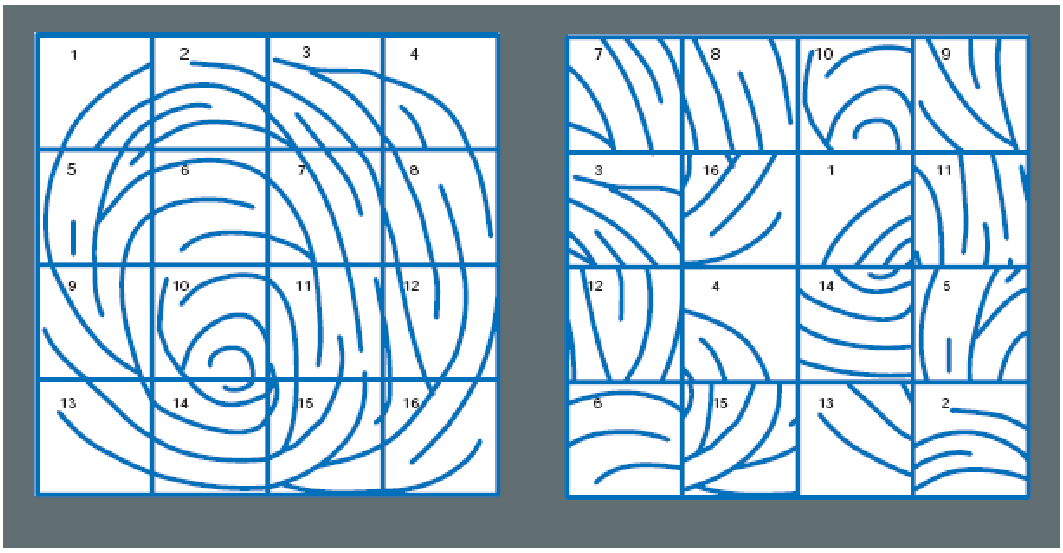


FIGURE (5). Distortions transform using block scrambling [5]

The representing blocks are jumbled repeatedly. Another example as shown by **[12] and [13].** The example of such a transform is shown in figures (6) which use more brute forces strength. The left blocks are unevenly mapped onto the right blocks, where multiple blocks are marked onto the same block. These transforms are not transferrable and therefore the original information can not be recovered from the distorted vision. Like it is difficult to say which of the two blocks, the point's inn compound block B, D basically came from. It is important that for the biometric transform to be reputable, the need is to get a biometric signal before transformation.

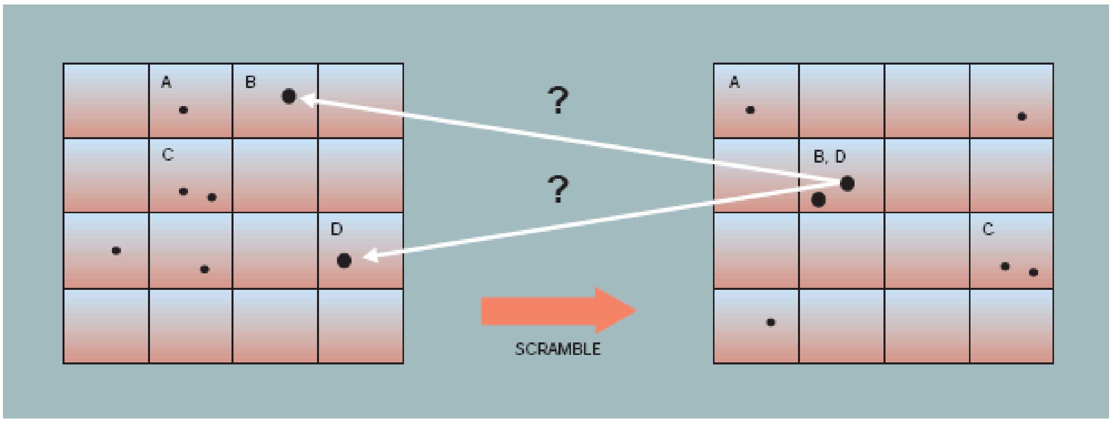


FIGURE (6). Distortion transform based o feature perturbation[5]

Here is an example of an of a non transferrable transform of a point pattern.

$D=\{(x_i,y_i,\theta_i),\ i=1,\ldots\ldots.H\}$…………………………………..(1)

D can not be retransformed from S`

$D=\{(x_i,y_i,\theta_i),\ i=1,\ldots\ldots..H\}\ \rightarrow S`$…………………………..(2)

$=\{(X_i,Y_i,\Theta_i),\ i=1,\ldots\ldots\ldots.H\}$……………………………(3)

X coordinates of the set D can be renovated via a mapping x→X, or X=F(x)

$X=F(x) = {}_{n=0}\Sigma^{N}a_n\, x^{n}={}_{n=0}\prod^{N}(x-\beta_n)$…………………………(4)

Similarly non-transferable polynomial transforms:

$Y=J(y)$ and $\Theta=I\ (\theta)$…………………………… ………..(5)

2.2 FACE RECOGNITION AUTHENTICATION

This is shown by [2], Cancellable biometric has to be transformed into one way sense in order to protect the biometric data firstly the co-occurrence matrix is computed with the original face image. Then to transfer the image within a non-linear transformation, the original face image is passed through a non linear transformation, which involves polynomial computation and dynamic software manipulation of the polynomial output. The non-zero co-occurrence vector can be extracted form computed co-occurrence matrix which will then used to construct the new co-occurrence matrix that is multiplied by the transformed image using hadamard product. The reason why these two stages combined is because to reduce correlation of the data samples and introduce outliners to it which helps to enlarge the face recognition, which will enhance the recognition performance, flexibility and enables wide range of manipulation.

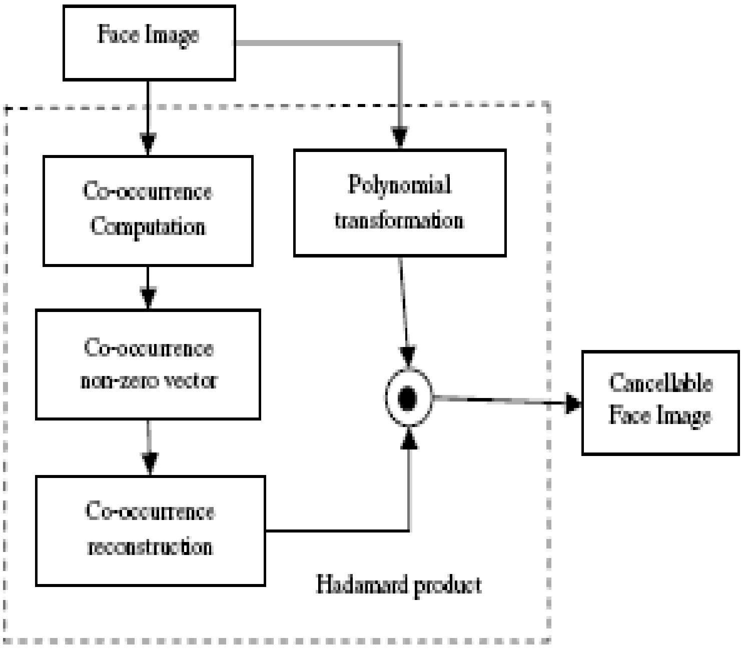

Face Image
Co-occurrence Computation
Polynomial transformation
Co-occurrence non-zero vector
Cancellable Face Image
Co-occurrence reconstruction
Hadamard product

FIGURE (7). Procedure of producing cancellable transformed image [2]

A. non-linear/polynomial transformation (stage I)

Polynomial functions of higher order are one way transformation which is hard to invert to its original form. Let f (.) donates a n order polynomial function and X is input sequence that shows the coordinates of the original image, will be generated by the polynomial. Through the polynomial function every coordinate is transformed into another coordinates.

$$F(x)= {}_{i=0}\Sigma^{n} b_i \, x^i \qquad (6)$$

By the polynomial function (6), the transformed value f(x) would have more than a single x value. According to worse condition, i.e. with the lowest security, the possible values for each transformed sample:

$$f^{-1}(f(x))=x_1 \quad \text{or} \quad f^{-1}(f(x))= x_2 \qquad (7)$$

The image has a matrix K*f. the image is vectorised into one vector that has K*F dimensions for simplifications.

$$\{X_1, x_2, x_3, \ldots\ldots x_{K*F}\} \in X \qquad (8)$$

Where X is the image and x_i (i=1,2,3,….K*F)are the samples of the image . Therefore,

$$\{f(x_1),f(x_2,)f(x_3)\ldots\ldots f(x_{K*F})\} \in f(X)=C \qquad (9)$$

Where C is the transferred image

From (7) the worse case, the possibility of each f(x) is two. Therefore the probability of occurrence if P (F(x)) =0.5. So P(C) =0.5K*F is the joint probability where K*F is usually a very large number.

Let us suppose that the number of reversing possibilities of each f(x) is k in order to extend the solution.

$$P(f(x)) = 1/k \qquad (10)$$

$$\text{So } P(C) = (1/k)\ K*F \qquad (11)$$

Hence P(C) is very small which means high irreversibility.

B. Co-occurrence Matrices (Stage II)

The use of this matrix is due to the fact that they could represent the image in terms of pixels relationship these matrices are derived from grey levels of image.

$$Cd;\theta[i,j] =|\{m,c\} \quad | \qquad (12)$$

$$|\{I[m,c]= i\wedge I[m+d\cos(\theta), c+d\sin(\theta)]=j \}|$$

Where I[m,c] is the intensity at location (m,c) and (d,θ) are distance and the orientation of the displacement vector as shown by [2]. A square matrix of L*L is computed using equations (12)[1], where L is the number of the grey levels. To reconstruct K*F matrix, this non zero co-occurrence is used, where K and F are the original image dimensions.

C. Recognition with 2D-PCA

2DPCA instead of operating on vectors in PCA operates on matrices. Equation (13) is the covariance matrix, where E[.] is te expected value and total scatter is equation (14).

$$S_x=E[(B-EB)X][(B-EB)X]^T \qquad (13)$$

$$Tr(S_x)= X^T [E(B-EB)^T][(B-EB)]X \qquad (14)$$

Therefore the generalised scatter criterion:

$$P(X)= XTGtX \qquad (15)$$

$$G_t= i/M\Sigma_{j=1}^{M}(Bj-B^{-})^T (Aj-B^{-}) \qquad (16)$$

Let $\tilde{\tilde{A}}$ denotes the cancellable biometric face, V the reconstructed matrix and Á is nonlinearly transformed face as shown below:

$$\tilde{\tilde{A}}= \acute{A}^{\circ}V=f\,(A)^{\circ}\ V \qquad (17)$$

Where both matrices shave same dimensions K*F and ° is the Hadamard Product. The covariance is given by

$$R_t= E[(\tilde{\tilde{A}}-E\ \tilde{\tilde{A}})(\ \tilde{\tilde{A}}-E\ \tilde{\tilde{A}})] \qquad (18)$$

Therefore

$$R_t = \mathrm{cov}(\acute{A})\circ\mathrm{cov}(V)\text{-}E\ \acute{A}^T E\ \acute{A}\circ EV^T EV\text{-}E\acute{A}\ E\acute{A}\circ EV^T\ EQ \qquad (19)$$

From (19) the covariance matrix consists of the co-occurrence matrices and covariance matrices of the transformed face images that are multiplied using the Hadamard Product.

2.1.3 Hadamard codes

This is shown by [14] that A Hadamard code is generated by the Hadamard matrix, i.e. a square orthogonal matrix with elements 1 and -1. Orthogonality says the inner product of any two distinct rows or columns is always 0 and the size of the this matrix must be {1, 2,4m} for natural numbers m. there are several ways to generate Hadamard matrices ….

The simplest Hadamard matrix is whose order i.e. k=1, is by [14]

$$H_1 = \begin{bmatrix} + & + \\ + & - \end{bmatrix}$$

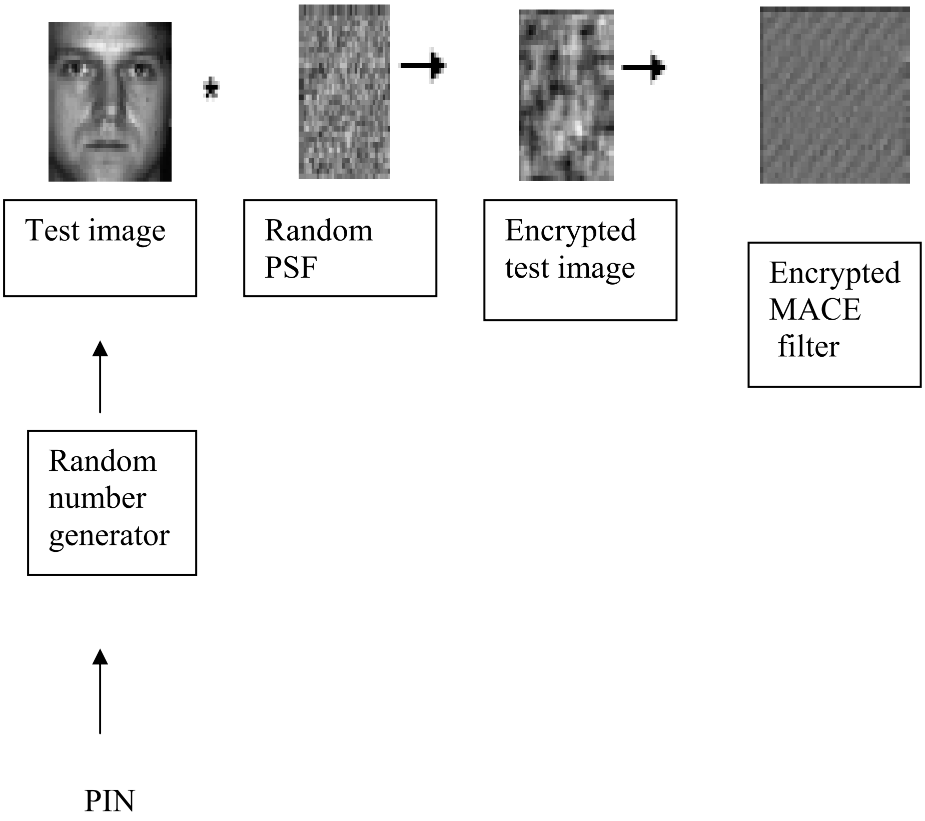
.

2.3 FACE RECOGNITION USING CANCELLABLE BIOMETRIC FILTERS

2.3.1 SYSTEM ARCHITECTURE

This has been shown by [15] that identical performance is obtained from minimum average correlation energy (MACE) filters even when the training images are convolved with a random kernel for biometric authentication. The figure shows the system architecture which shows the enrolment stage for encrypted filters.

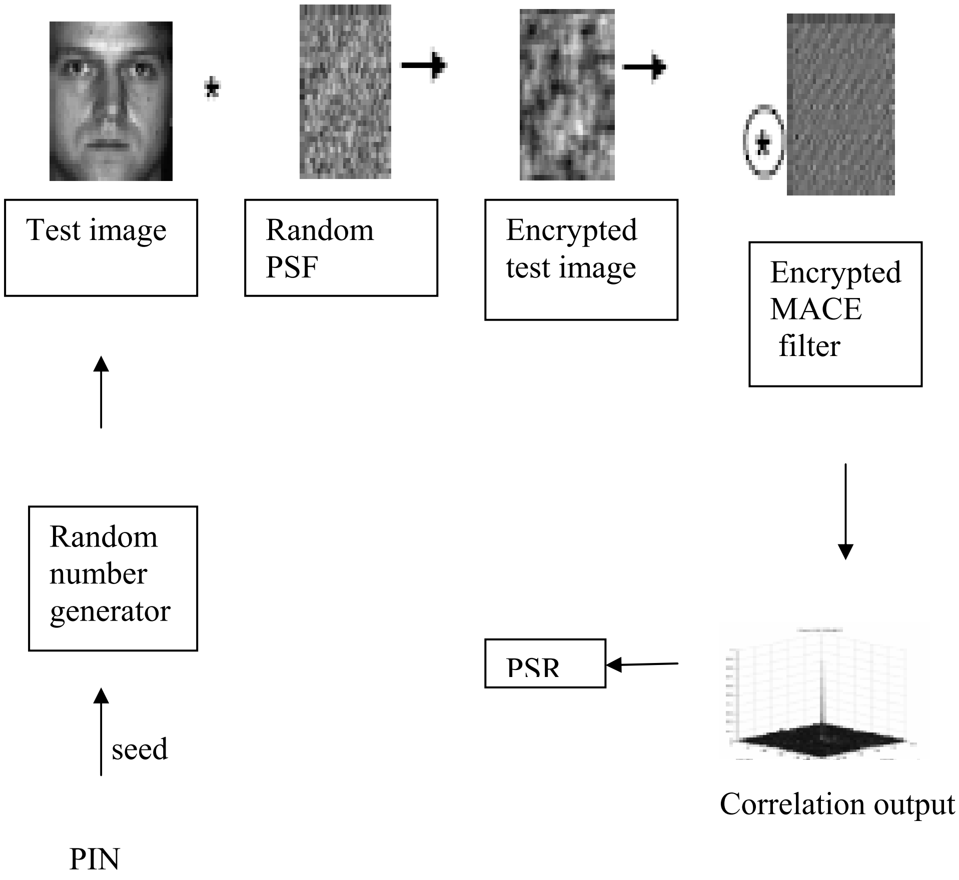
FIGURE (8). Enrollment stage for encrypted filters**. [15]**



At the time of enrolment, new image of the user are taken and the images are then convolved with random convolution kernel. Now assume a PIN number which is taken as the seed in a random number generator which is then used to generate random convolution kernel. Then the single biometric filter is obtained from the convolved training images. The inverse Fourier transform can be done because of the convolution with random kernels. Then this resulting encrypted filter can be stored for authentication process. If any case the card is stolen or lost a different encrypted biometric filter can be synthesized using the enrolment system that generates a different convolution kernel. The important point is that the entire authentication process is performed in the encrypted domain. The figure shows the authentication stage for encrypted filters as shown below:

2.3.2 AUTHENTICATION STAGE

FIGURE (9). Authentication stage for encrypted filters. **[16]**



The peak to side lobe ratio (PSR) defined as (peak-mean)/STD where the mean and the standard deviation are computed in an annular region centred at the peak. This is shown by [16] that the standard difference between MACE filters and standard filter is that MACE is made of many training images where as the standard matched filter is made of a training image. These MACE filters also minimize the average correlation energy (ACE) resulting with sharp outputs and value non zero. The MACE filters thus are highly discriminative. The MACE filter in frequency domain is given by:

$$l= D^{-1}X(X^{+1}D^{-1}X)^{-1}c \qquad (20)$$

, Where X is the K×F matrix for N training images. C is the N×1column vector, D is a diagonal matrix containing the average power spectrum of all training images along its diagonal and h is the column vector.

The average correlation energy obtained with encrypted training images is same as the average correlation energy E of the MACE filter.

2.4 APPEARANCE BASED FACE RECOGNITION

This method is shown by [15] which use random kernels and MACE eighenface algorithm to find vectors for dimensionality reduction by using the PCA (Proposed Component Analysis). PCA is a method which represents a collection of sampled data. ICA is similar to PCA except that the distribution of the components is organised to be non-Gaussian. ICA means Independent Component Analysis [17]. The below figure describes the facial representation of both PCA and ICA.

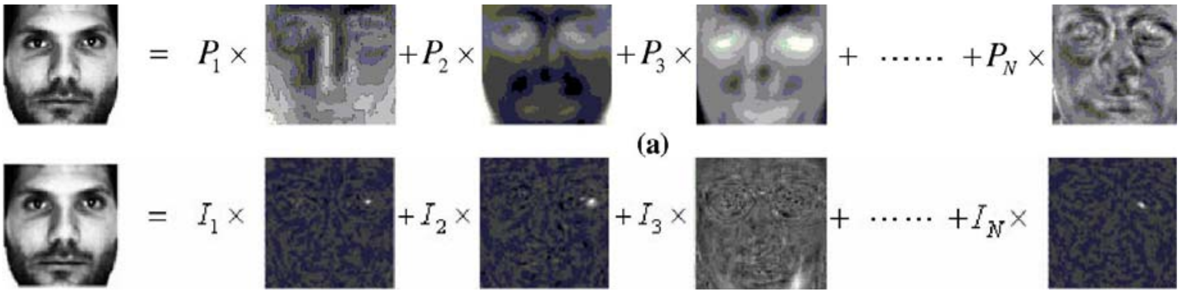

= P_1 × + P_2 × + P_3 × + ... + P_N ×
(a)
= I_1 × + I_2 × + I_3 × + ... + I_N ×

FIGURE (10). Facial representation using PCA and ICA **[15]**

The figure below shows the overall procedure of Proposed Component Method.

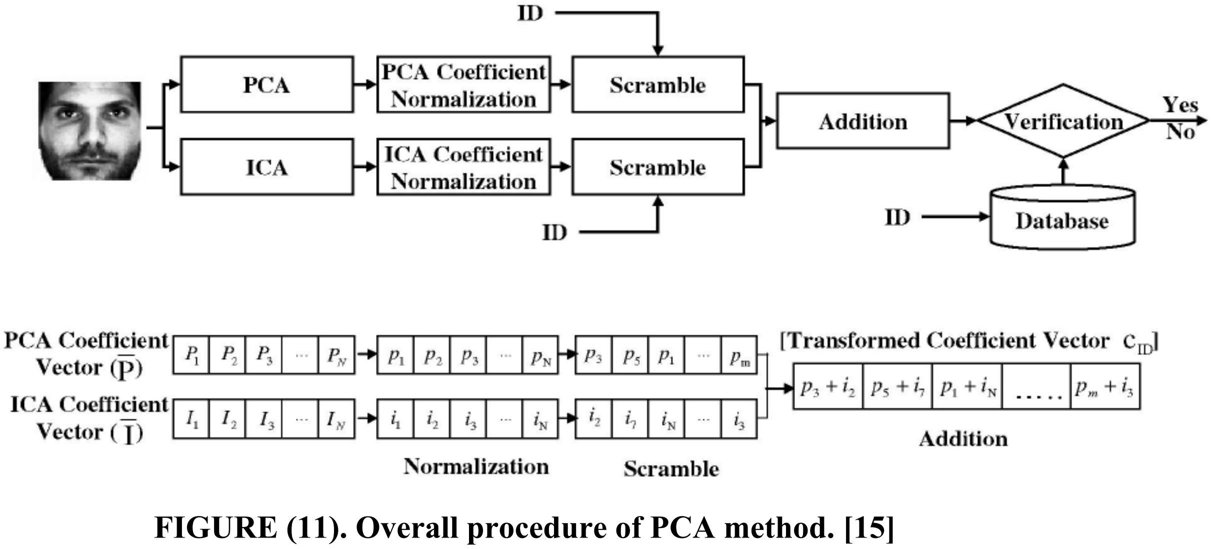

ID
PCA
PCA Coefficient Normalization
Scramble
ICA
ICA Coefficient Normalization
Scramble
ID
Addition
Verification
Yes
No
ID
Database
PCA Coefficient Vector ($\overline{P}$)
P_1 P_2 P_3 ··· P_N
p_1 p_2 p_3 ··· p_N
p_3 p_5 p_1 ··· p_m
ICA Coefficient Vector ($\overline{I}$)
I_1 I_2 I_3 ··· I_N
i_1 i_2 i_3 ··· i_N
i_2 i_7 i_N ··· i_3
[Transformed Coefficient Vector c_{ID}]
p_3+i_2 p_5+i_7 p_1+i_N ..... p_m+i_3
Normalization
Scramble
Addition

FIGURE (11). Overall procedure of PCA method. [15]

The basic idea of PCA method is to generate coefficients by adding the coefficients of scrambled PCA and ICA coefficients.

1. **NORMALISATION**

n- Dimensional PCA coefficient vector as shown by [15].

$$P^{-} = [P_1,P_2,P_3,\ldots\ldots,P_N] \qquad (21)$$

And ICA coefficients vector

$I^{-} = [I_1,I_2,I_3,\ldots\ldots,I_N]$, they both extracted from the input face image.

The two coefficients are normalised using their norm is given as follows:

$$P= P^{-} /|P^{-}|=^{-} [P_1,P_2,P_3,\ldots\ldots,P_N] \qquad (22)$$

$$I= I^{-} /|I^{-}|=^{-} [I_1,I_2,I_3,\ldots\ldots,I_N] \qquad (23)$$

Here P^{-} and I^{-}, Shows the L2 norm of vector

2. **Scrambling Normalisation Vector Coefficient**

Each coefficient vector is unevenly scrambled and two scrambling functions ${}_{ID}S^{PCA}(\bullet)$ and ${}_{ID}Z^{ICA}(\bullet)$. ${}_{ID}S^{PCA}(\bullet)$, this is the function for shuffling the normalised PCA coefficient vector p, and ${}_{ID}Z^{ICA}(\bullet)$ is a function for muddling the normalised coefficient vector i. the shuffled PCA and ICA coefficients are as shown by [15] :

$$P_s= {}_{ID}S^{PCA}(p) \qquad (24)$$

$$I_s= {}_{ID}Z^{ICA}(p)\# \qquad (25)$$

New transformed coefficients are made by mishmash rule associated with the ID or by replacing the ID i.e. used id.

3. **Addition of Normalised Coefficient Vectors**

Transformed coefficient vector can be produced by the addition of PCA and ICA scrambled coefficient vectors is as shown by [15]:

$$C_{ID}= \partial p^s+\beta i^s \qquad (26)$$

And $\partial = \beta= 1$

2.5 BIOPHASOR

This is as shown by [18] Biometric characteristics are invariant and to fix this problem, biophasors are implemented. Biophasor is a set of binary code based on the common mixing between the user specific tokenised pseudo random number and the biometric feature [18]. Biophasor method enables the reoccurrence of biometric template through token replacement. The Biophasor transformation is non transferable to its original form and has a extremely low error rate. The main objectives of this method are two overlaps: to see which Biometrics template can be reused by replacing the token when it is composed. And the other is this transformation is non transferable and has less error rate and does not leak information. Biophasor has the ability to reduces intra class and enlarge inter-class variation which causes less error rate equal to zero.

2.6 BIOHASHING

The Cancellable Biometrics was discoursed by [19] who imported a technique which known as Biohashing. This is the combination of the biometric template and a set of user-specific tokenised random number (TRN) to give a set of non-invertible binary bit strings. Biophasor method gives zero error performance when legitimate token was used. Biohashing is defined as follows by [19]:

a) Feature Extraction: This technique is used to extract the biometric feature which is expressed in a vector form; $\Gamma \in R^{n.}$ where n is the feature length.

b) Apply a token to generate m orthogonal pseudo random vectors, $\{r^{\perp} i R^{n} | i=1, \ldots.. m\}$ and $m <= n$.

c) Enumerate $\{(\Gamma | r^{\perp}) | i=1, \ldots\ldots. m\}$ where () indicates inner product operation.

d) Calculate an m bit Biohash template, $b= \{bi | i=1, \ldots\ldots m\}$ from

$$Bi = \{0 \text{ if } (\Gamma | r^{\perp} i) <= \tau \qquad (27)$$
$$\{1 \text{ if } (\Gamma | r^{\perp} i) > \tau$$

The Biohash template can be put in the centred database when enrolment is done for implementation purpose. At the verification stage, the selected feature image is fused with the legitimate random number and the subsequent Biohash is analyzed with the obtained template using hamming distance i.e. the difference in number of bits.

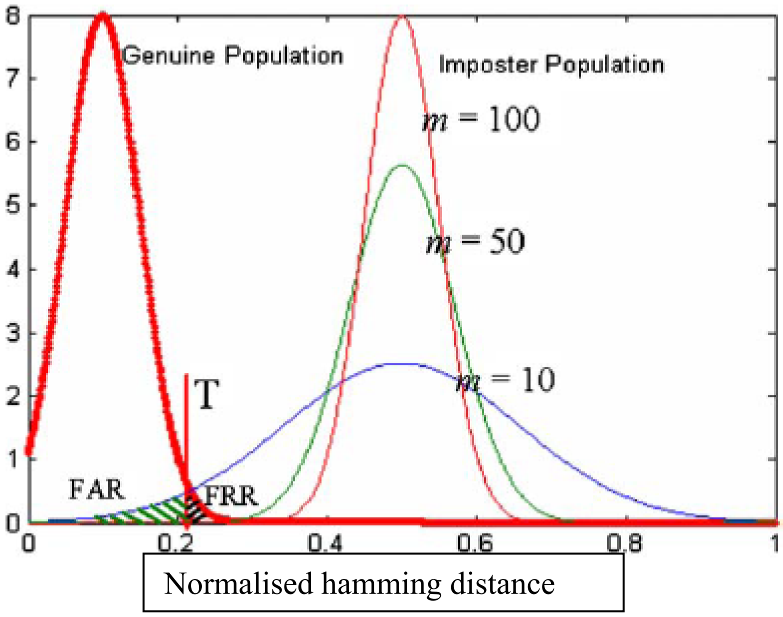
In general Biohash if formulated as shown by [19]

$b=Sig\ ({}_{k}\Sigma \Gamma_{k} r^{\perp} - \tau)$ or $b= Sig(RT-\tau)$, where Sig(.)m is known as signum function and τ is a preset threshold, which is normally set to $\tau=0$.

2.6.1 BIOHASH’S STATISTICAL CHARACTERISTICS

The actual imposter for biohash is shown in **FIGURE (12)**, **[20]**

FIGURE(12). Actual characteristics of Biohash, [20]



The biohash characteristics increase as m goes up. As higher value of m it is clearly shown that the biohash can get zero error rates i.e. FAR=FRR = zero%.

2.1.7 Random multispace quantisation (RMQ)

RMQ consists of: feature extraction, random multispace mapping, and quantisation, as shown by [21]. In the first stage the biometric image is transformed linearly using fisher discrimination analysis (FDA) then the sequence of random subspaces is obtained by mapping the biometric feature vector. If an third person is trying to recover the biometric information have to invert the random multispace quantisation process.

Feature extraction

Fisher discrimination analysis (FDA) is a accepted technique to increase the ratio of the interclass to the intraclass disperse. The fisher discrimination projection is shown as:

$$G_k= v^T(e_s-e^-), \text{ here } s =1,\ldots\ldots\ldots c-1 \qquad (28)$$

FDA can be debugged through the following steps:

1) PCA [22], ending in less dimensionality.
2) FDA in the lowered PCA eigenspace.

Ranbdom mapping

In this stage remapping is done on to a random subspace by face feature as follows:

$$Y=nH_{pm}^T w_p \qquad (29)$$

Where $n=(p/m)^{1/2}$ and $m<=p$

Johnson-lindenstrauss (J-L) Lemma:

This is shown by [23] that for either $0<\varepsilon<1$and any integer d , suppose p be a positive integer such that $p\geq 4\text{ld } d / \varepsilon^2/2- \varepsilon^3/3$.

Quantisation:

The last step is to quantize the random multispace outcomes. Binarisation is processed through the assessment of all u_k against some empirical threshold value Γ and debugging the collective outcomes to compose bitstring b. This authentication is the misstep to daugman irisCode **[24]**.

DISCUSSION

To realise cancellable biometrics face in practice there are many techniques like morphing, Biophasor, Biohashing and Random Multispace Quantisation. Although they all are known for enhancing security, performance and non-inveretibility, but these techniques have advantages and disadvantages.

Morphing, the first proposed method for authentication of cancellable biometrics has a low false rejection rate and false acceptance rate. Operating point is set depending on the applications requirements and at that point the FAR and FRR rates can be different.

Biophasor uses the missing of biometric template and pseudo random number. Biophasor do not have good performance characteristics. Moreover with absence of PRN, biometric suffers form security invasion issues which is main concern for us, even it property of revocable is also deteriorated.

Biohashing has the poorer performance than biophasors and like biophasors it also suffers from privacy issues and the property of non-revocability.

Although RMQ has a good performance but it also suffers privacy problems and also non-revocability when external input is not provided. and do not give the actual results.

CONCLUSION

After the careful investigation of the previous research on cancellable biometrics face, conclusion reaches to the point that morphing technique has the higher ability to perform accurately and has less false rejection rate and false acceptance rate , and has a enhanced security regarding biometric information. In morphing, it is shown that if a one error rate is reduced then the other error rate will automatically go up. Morphing implements the block scrambling which scrambles the biometric and that data is revocable.

Morphing can be considered as an important candidate to realise cancellable biometrics systems in this world where the need of privacy is increasing.

REFERENCES

1) R.M. Bolle, J.H. Connell and N.K. Ratha "Biometric Perils & Patches" Pattern Recognition, vol 35 pp. 2727-2738,2002.
2) M.A. Dabbah, W.L. Woo, S.S. D Lay," proceeding of the 2007 IEEE Symposium on Computational Intelligence in Image and Signal Processing pp.121-126 (CIISP 2007).
3) R. Chellappa, C.L. Wilson and S. Surohey,"Human and Machine Recognition Of Faces : A Survey" Proceedings Of The IEEE , volume 83 pp. 705-741, 1995.
4) A. Goh, D. C. L. Ngo, "Computation Of Cryptographic Keys From The Face Biometrics," International Federation For Information Processing 2003, Springer verlag lncs 2828, pp.1-13 ,2003.
5) N. K. Ratha, J. H. Connell and R. M. Bolle," Enhancing Security and Privacy In Biometric Based Authentication Systems" "IBM Systems Journal vol.40 pp614-634, 2001.
6) A. B. J. Teoh and D. C. L. Ngo," Cancellable Biometrics Featuring with TRN, Pattern Recognition" vol.26 pp. 1454-1460, 2005.
7) D. Maltoni , D. Maio, A. K. Jain and S. Prabhakar ," Handbook Of Fingerprint Recognition, pp.301,307, springer 2003.
8) B. J. A. Teoh and C.L. D. Ngo,"Cancellable Biometrics Featuring with Tokenised Random Number" Pattern Recognition Letters" vol.26 no. 10, pp. 14554-1460 2005.
9) B. J. A. Teoh,C. L. D. Ngo and A. Goh ,"Personalised Cryptographic Key Generation Based on Facehashing" Computers and Security j, vol.23 no.7, pp. 606-614, 2004.
10) W. K. Yip, A. Goh, B. J. A. Teoh and C. L. D. Ngo," Cryptographic Keys from Dynamic Hand Signature with Biometric Secrecy Preservation and Replacibilty " Proceeding fourth IEEE Workshop Automatic Identification Advanced Tech. pp.27-32, 2005.
11) M. Savvides and B. Kumar and B.K. Khosla "Cancellable Biometrics Filters For Face Recognition" International Proceedings of 17th International Conference on Pattern Recognition; Alanitos, IEEE Computer Society; pp. 922-925 2004.
12) G. Wolbeg,"Image Morphing:A survey,"The Visual Computer 14,PP.360-372(1998**)**.
13) T. Beier and S. Neely,"Feature Based Image Metamorphosis,"Proceedings of SIGGRAPH, ACM, NEW york(1992), pp.35-42.
14) Feng Hao, Ross Anderson, John Daugman," Combining Cryptography with Biometric Effectively. July 2005 pp1-17 Technical Reports Published by university of Cambridge.
15) Maris Savvides, B. V. K. Vijaya Kumar and P. K. Khosla "Cancellable Biometric for Face Recognition," Proceedings of the 17th International Conference on Pattern Recognition , pp. 1054-4651 2004.
16) A. Vanderlugt, " Signal Detection by Complex Spatila Filtering " IEEE Trans. Inf. Theory pp139-145, 1992.
17) M. S. Bartlett, J. R. Movellan, and T. J. Sejnowski, " Face Recognition by ICA ," IEEE Trans. Neural networks , vol. 13 , no.6 , pp1450-1464,2002

18) Andrew B J Teoh and David CL Ngo “Biophasor: Token Supplemented Cancellable Biometrics”PP.1-5, 2006.
19) T. Connie, A. Teoh, M. Goh, D. Ngo, Palmhashing: A Novel Approach to Biometrics, Information Processing Letters 93(1), (2004)PP.1-5.
20) J. Daugman, “The Important of Being Random: Statistical Principles of Iris Rcognition, Pattern Recognition 36(2003)279-291.
21) Andrew B.J. Teoh , Member, IEEE Alwyn Goh and David C.L. Ngo,IEEE,Random Multispace Quantisation as an Analytic Mechanism for Biohashing of Biometric and random identity inputs,”IEEE transactions on Pattern Analysis And Machine Intelligence , vol.28.no.12, pp 1892-1901, Dec. 2006.
22) M. Turk and A. Pentland,”Eigenfaces for Recognition,” J. Cognitive Neuroscience, vol. 3, no.1, pp 71-86,1991.
23) W. B. Johnson and J. Lindenstrauss,” Extension of Lipschitz Mapping Into a Hilbert Space,” Proc. Conf. Modern Analysis and Probability, pp. 189-206, 1984.
24) J. Daugman ,” The Importance of Being Random: Statistical Principles of Iris Recognition ,” Pattern Recognition vol.36, no.2 pp279-291, 2003.