Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Image and Signal Processing (CIISP 2007)

Secure Authentication for Face Recognition

M. A. Dabbah, W. L. Woo and S. S. Dlay
The School of Electrical, Electronic and Computer Engineering
Newcastle University
Newcastle upon Tyne, NE1 7RU, United Kingdom
{m.a.dabbah, w.l.woo, s.s.dlay}@newcastle.ac.uk

Abstract - **In this paper, we present a new technique to protect the face biometric during recognition, using the so called cancellable biometric. The technique is based on image-based (statistical) face recognition using the 2DPCA algorithm. The biometric data is transformed to its cancellable domain using polynomial functions and co-occurrence matrices. Original facial images are transformed non-linearly by a polynomial function whose parameters can be change accordingly to the issuing version of the secure cancellable template. Co-occurrence matrices are also used in the transform to generate a distinctive feature vector which is used for both security and recognition accuracy. The Hadamard product is used to construct the final cancellable template. It shows high flexibility in proving a new relationship between two independent covariance matrices, which is mathematically proven. The generated cancellable templates are used in the same fashion as the original facial images. The 2DPCA recognition algorithm has been used without any changes; the transformations are applied on the input images only and yet with higher recognition accuracy. Theoretical and experimental results have shown high irreversibility of data with improved accuracy of up to 3% from the original data.**

I. INTRODUCTION

A biometric authentication system is a system that relies on the physical feature of the human body for identification. It is a system that is challenging the fatal problems in traditional authentication systems, such as PIN and token systems. Biometric is defined as a unique physical characteristic of the human body that can be used to verify the identity. It must be unique, permanent and universal for a well performance application such as face, iris, retina, fingerprint just to name a few. Face recognition is one of the mostly used biometrics. Many approaches and methodologies have been previously proposed, which can be categorised as, feature-based and image-based, [1]. Feature-based approaches are dependant on predefined features in the human face that can be used to distinctively identify the person. This approach has dominates in the past decades before the image-base approach was proposed. The image-based approaches are operating on the actual face image for recognition instead of the extracted features and templates in the feature-based, hence the name image-based. Their core processing procedures rely on the statistics of the facial appearance (they are sometimes called statistical-approaches), such as multivariate analysis. They are also called eigenface approaches, which have been intensively used in different face recognition systems and methods; they were extended to a number of different methods [2], such as FLD, FFC, KFD and KPCA. They are preferred to the other technique due to their analytical mathematical-base and high recognition accuracy. Although face recognition and other biometrical authentication have recently re-emerged with further development and improvement, there still exists a significant and fatal security problem in biometric systems. Biometric information is not protected and if it is compromised during any stage in the processing chain, the privacy of such data is lost and can not be used again as an identity. This is due the permanence of biometrics since they should remain unchanged over the lifetime of the individual to maintain high reliability for recognition. Cancellable biometric protects the biometric data by transforming the data into other domain (cancellable domain), where data cannot be inverse transformed to its original form. Recognition is conducted in the transform domain, which protects the data over the entire processing chain, hence the cancellable biometric should be suitable to perform accurate recognition. In addition, cancellable biometric enables the facility of regenerating different cancellable template of the original biometric when the previous one is compromised.

The concept of cancellable biometric was first proposed by [3]. Several methods for generating cancellable biometrics have been proposed. The main idea behind cancellable biometric is to transform the original data to a certain domain, where recognition can be accurately performed, and cannot be retransformed back to the original data. The method in [4] introduces an approach that is based on tokenised pseudo-random number and Wavelet Fourier-Mellin Transform framework (WFMT) for face recognition system. The method is composed from two components, generation of invariant and discriminative face feature with moderate degree of offset using the WFMT, and to attain the FaceHash by a serial number goes through a discretisation process. This number is obtained from an iterated inner product operation between face features and random numbers. In [5] the cancellable biometric is generated by encrypting a training set of images to construct a minimum average correlation energy filter for face authentication. The filter is convolved with the original biometric to produce the cancellable template. Cancellable biometric templates are reproduced from the original biometric by changing the convolution kernels of the filter. Cancellable biometric could be defined as intentional repeatable distortion of a biometrics signal based on chosen transforms [3, 6]. The distortion is repeated in the same fashion during enrolment and for every subsequent authentication. For face recognition, a morphed image is enrolled. This morphing is achieved by a regular point pattern or grid that are overlaid on the image after transforming the face image into canonical position.

In this paper we present a novel cancellable protection method to the biometric information that guarantees both security and high recognition accuracy. We will also present details analysis on the characteristics of cancellable biometric and how it affects the recognition performance and accuracy.

II. CANCELLABLE BIOMETRIC

Original biometric such as face, fingerprint or iris cannot be cancelled or replaced by another one. To protect the biometric information, the cancellable version of the biometric has to be transformed in one-way sense. One way transformation is an open problem in mathematics, where $f^{-1}(f(x)) = x$ provided that $f^{-1}(\cdot)$ exits. Considering the strong one-way function, this function can be easily computed but hard to invert. Hence, if x is an input to this function $f(\cdot)$, the output y is computed in a polynomial-time algorithm. On the other hand, this function is hard to invert in that any probabilistic polynomial-time algorithm could succeed to compute x when y is given with a negligible probability [7]. Recognition should be conducted in the cancellable domain therefore, the domain have to be suitable for accurate recognition performance. Conducting the recognition in the cancellable domain is the major concept of security in the entire system. It protects the biometric data at any stage of the recognition process and if any information is compromised, it is going to be the cancellable version of the information that can be cancelled. In addition, the reason of calling cancellable biometric like that is the possibility that it provides to cancel the template of the biometric that is used for the recognition when they are compromised by impostors, fig. 1.

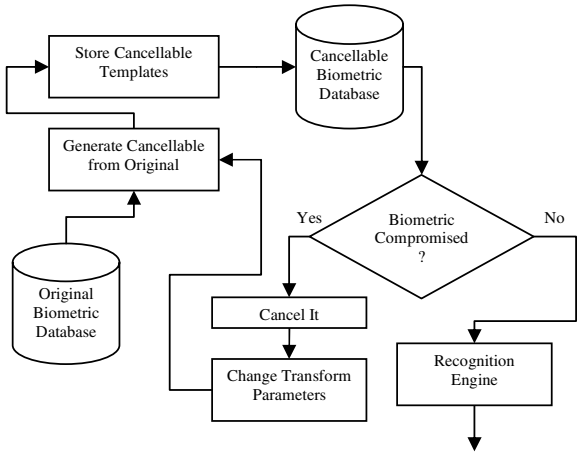

Fig. 1: reissuing new cancellable template when the previous one is comprised.

From the original biometric a number of cancellable biometric templates should be able to be regenerated, the larger the number, the better. This purports that biometric information of the human body to be abundant or endless. The proposed cancellable transformation is designed for image-based face recognition systems in general. Image-based recognition engines have been intensively used and well establish research. A significant improvement was achieved when the eigenfaces method was proposed [8] in the early 90's. They proved their accuracy, efficiency and their good performance under difficult acquisition conditions specially the 2DPCA projection method [9].

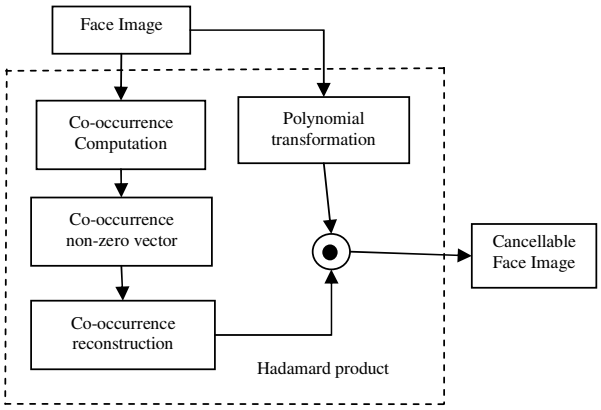

Fig. 2: procedure of producing the cancellable transformed image.

The cancellable transformation is established in several stages, fig. 2. First, the co-occurrence matrix is computed from the original face image. Then the original face image is passed through a non-linear transformation that transfers the image within a very non-linear mechanism, which involves polynomial computation and dynamical software manipulation of the polynomial output. The computed co-occurrence matrix is then used to extract the non-zero co-occurrence vector, which will construct the new co-occurrence matrix that is multiplied by the transformed image using the Hadamard product. The reason of combining these two stages is to reduce the correlation of the data samples and introduce outliers to it, which enlarge the recognition space in the face recognition system, hence better discrimination and separation between classes that leads to higher recognition accuracy rate. The Hadamard product is an element-wise multiplication of vectors and matrices. It provides good flexibility in the product term, which enables wide range of manipulation. It establishes an important relationship within the cancellable biometric data by the joint-probability of two covariance matrices as discussed later in this section.

A. Non-linear\Polynomial Transformation (Stage I)

Using polynomial function, new coordinates of the image are introduced. Polynomial functions of a high order are one-way functions that are hard to invert in polynomial-time algorithm when the input is of a large sequence. Let $f(\cdot)$ donates a n order polynomial function and X is the input sequence that presents the coordinates of the original image. A new coordinates, Y that represents the image, will be generated by the polynomial. Each coordinate in the image is transferred to another coordinates through the polynomial function. This transformation will not change the intensity values of the pixels

themselves, which will retain the recognition accuracy using the image-based approaches, such as 2DPCA, unchanged as has been practically proved. The transformed images do not resemble any facial characteristics at all. In fact, they appear as a random data. Polynomial function used for transformation has a certain number of parameters. In tern, these parameters determine the new transformation characteristics.

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad (1)$$

By the polynomial function (1), the transformed value $f(x)$ would have more than a single x value. According to the worse case scenario i.e. with the lowest security, there are two possible values of each transformed sample:

$$f^{-1}(f(x)) = x_1 \quad \text{or} \quad f^{-1}(f(x)) = x_2 \quad (2)$$

The image has a matrix size MxN. For simplification, the image is vectorised into one vector that has MxN dimensions.

$$\{x_1, x_2, x_3, x_4, x_5 \ldots x_{MxN}\} \in X \quad (3)$$

Where X is the image and $x_i \quad (i = 1,2,3,\ldots,MxN)$ are the samples of this image. Hence,

$$\{f(x_1), f(x_2), f(x_3), \ldots, f(x_{MxN})\} \in f(X) = C \quad (4)$$

Where C is the transferred image in the cancellable domain.

From (2), the worse case scenario, the possibility for each $f(x)$ is two. Hence the probability of occurrence is $P(f(x)) = 0.5$. It follows that $P(C) = 0.5^{MxN}$ is the joint probability where MxN is usually a very large number (in the order of thousands).

In order to extend this solution, let us assume that the number of reversing possibilities of each $f(x)$ is k.

$$\therefore \quad P(f(x)) = 1/k \quad (5)$$

And $$P(C) = (1/k)^{MxN} \quad (6)$$

It is very clear from the final solution that $P(C)$ is very small, which contributes to a very high irreversibility.

B. Co-occurrence Matrices (Stage II)

The use of the co-occurrence matrices is due to the fact that they could represent the image in terms of pixels' relationship. Co-occurrence matrices are derived from the grey levels of the image. It is a second order statistic that measures relationships of grey levels in the image by indicating the joint probability of them at a certain displacement (distance and orientation) in the image [10, 11].

$$C_{d;\theta}[i,j] = \left| \begin{Bmatrix} [r,c] | \\ I[r,c] = i \,\hat{}\, I[r + d\cos(\theta), c + d\sin(\theta)] = j \end{Bmatrix} \right| \quad (7)$$

Where $I[r,c]$ is the intensity at location (r,c) and (d,θ) are the distance and the orientation respectively of the displacement vector that is also called the position operator. However, the co-occurrence matrix that we used is multiplied by the total number of pixel's parings in matrix; hence it is not a presentation of probability anymore. A square matrix of LxL is computed using (7) [12], where L is number of the grey levels. From this square matrix the non-zero values are extracted as a form of vector. This non-zero co-occurrence vector is then used to reconstruct MxN matrix, where M and N are the original image dimensions. If the non-zero vector happens to be smaller than the matrix of the image dimensions, a repeated pattern of the vector is used to fill the rest of the matrix.

C. Recognition with 2D-PCA

Two dimensional PCA is an extended version of the conventional PCA. 2DPCA operates on matrices instead of vector in PCA. The following algorithm is a summary of the 2DPCA, further information can be found in [9]. Equation (8) is the covariance matrix, where $E[\cdot]$ is the expected value, and its total scatter is (9). The generalised scatter criterion is (10), where G_t can be expressed as (11).

$$S_x = E[(A - EA)X][(A - EA)X]^T \quad (8)$$

$$tr(S_x) = X^T [E(A - EA)^T (A - EA)]X \quad (9)$$

Hence, the generalised scatter criterion:

$$J(X) = X^T G_t X \quad (10)$$

$$G_t = \frac{1}{M} \sum_{j=1}^{M} (A_j - \overline{A})^T (A_j - \overline{A}) \quad (11)$$

The distance between two feature matrices is computed by the Euclidean distance, donated by $d(B_i, B_j)$, where B is the feature matrix. Therefore, for the test sample B, if $d(B, B_l) = \min d(B, B_j)$ and $B_l \in \omega_k$, then $B \in \omega_k$, where ω_k is the face class.

Let A'' denotes the cancellable biometric face, Q the reconstructed co-occurrence matrix and A' the nonlinearly transformed face as shown below:

$$A'' = A' \circ Q = f(A) \circ Q \quad (12)$$

where both matrices Q and A' have the same dimensions MxN and "$\circ$" is the Hadamard product. The covariance of the cancellable biometric is given by

$$G_t = E[(A'' - EA'')^T (A'' - EA'')] \quad (13)$$

Since Q and A' are independent due some nonlinear transformations, it follows that

$$\begin{aligned} G_t &= E[(A' \circ Q - EA' \circ EQ)^T (A' \circ Q - EA' \circ EQ)] \\ &= \mathrm{cov}(A') \circ \mathrm{cov}(Q) - EA'^T EA' \circ EQ^T EQ \\ &\quad - EA' EA' \circ EQ^T EQ \end{aligned} \quad (14)$$

From (14), the covariance matrix of the cancellable biometric consists of the covariance matrices of the transformed face images and the co-occurrence matrices that are multiplied using the Hadamard product. This relates the variations over the face images with the variations over the co-occurrence matrices with each other. Dividing the covariance matrix by the total energy distribution of the transformed images and the co-occurrence matrices, will give the correlation matrix of the cancellable biometric, which clearly indicates the joint probability of the face images with its corresponding co-

occurrence matrix. Hence, the discrimination and the recognition of face rely in the relationships between the transformed faces and the co-occurrence matrices that surly are varying from one set to another. In addition, the fact that polynomial function is presence in the covariance matrix via the transformed image makes the accuracy dependent to some extent upon the certain polynomial transformations characteristics. Note that the co-occurrence matrix is computed for the original face image A before the non-linear transformation $f(\cdot)$.

And for classification, let Y'' donates the extracted features of the cancellable biometric face.

$$Y''_k = A'' X_k \tag{15}$$

$$B''_i = \left[Y''^{(i)}_1, Y''^{(i)}_2, Y''^{(i)}_3, \ldots, Y''^{(i)}_d\right] \tag{16}$$

$$B''_j = \left[Y''^{(j)}_1, Y''^{(j)}_2, Y''^{(j)}_3, \ldots, Y''^{(j)}_d\right] \tag{17}$$

$$d\left(B''_i, B''_j\right) = \sum_{k=1}^{d} \left\| Y''^{(i)}_k - Y''^{(j)}_k \right\|_2 \tag{18}$$

$$d\left(B''_i, B''_j\right) = \sum_{k=1}^{d} \sqrt{\sum_{l=1}^{m} \left(Q^{(i)}_l \circ \left(A'^{(i)}_l X_k\right) - Q^{(j)}_l \circ \left(A'^{(j)}_l X_k\right)\right)^2} \tag{19}$$

Using the Euclidean distance classifier, the results in (19) show that discrimination between different classes is affected by the co-occurrence matrices. This outlines a conditional restriction that relates variation in Q with variations in A'. Note that it does not relate Q to A' or via versa. Considering $A'^{(i)} X_k = V^{(i)}$ and $A'^{(j)} X_k = V^{(j)}$ are two large multidimensional vectors in the Hilbert space, and let $Q^{(i)}$ and $Q^{(j)}$ to be two different vectors that have the same dimensions in the Hilbert space, the probability of the convergence of the two vectors $V^{(i)}$ and $V^{(j)}$ to the exact same magnitude and angle, i.e. same point in the Hilbert space, if they are multiplied, using the Hadamard product, by the two other vectors $Q^{(i)}$ and $Q^{(j)}$ is very small in comparison with the probability of being different.

Let $P(\theta)$ be the probability of having the same angle, and $P(M)$ be the probability of having the same magnitude. The probability of both vectors to converge to the same point is $P(E)$.

$$P(E) = P(M)P(\theta) = \frac{1}{2\pi\sqrt{\sum_{i=0}^{mn} x^{2i}}} \tag{20}$$

Cleary $P(M)$ is very small and the probability $P(E)$ is even smaller when multiplied by $P(\theta)$ to verify the condition of having the same angle and magnitude.

III. Results and Discussion

The experiments were conducted on the ORL database [13]. It contains 40 classes with 10 acquisition of each subject i.e. 400 images in total. Each image is 112x92 pixels. The face images have been captured under different conditions, such as posture variations of the faces, facial expressions and facial wear. Each pixel has 8 bits to present the grey-level from 0 to 255. Samples of these images are shown in fig. 3. The first 5 images are used for training the algorithm and the rest 5 images are used to evaluate the algorithm.

Fig. 3: Four face images of the same subject from the ORL database

The proposed cancellable biometric images are presented in fig. 4. They do not look like face images or any other images at all. They do not contain any shape as the morphed images and look like a random sequence, which makes them misinterpreted by humans.

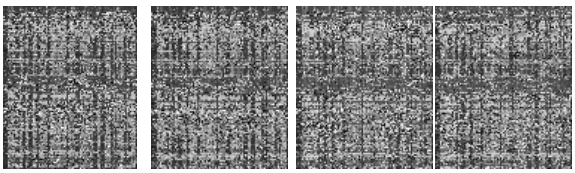

Fig. 4: cancellable face images of four different face images of the same subject in fig. 3.

As has been proved before, the irreversibility of the transformed images can be calculated according to the image size (112x92) together with the number of reversed values of each transformed pixel. Let us assume that each transformed pixel has at least 3 inverse transformed values i.e. $k = 3$. The estimated probability of reversing the cancellable biometric face to its original form using (6) is 5.53^{-4917}, which is extremely small.

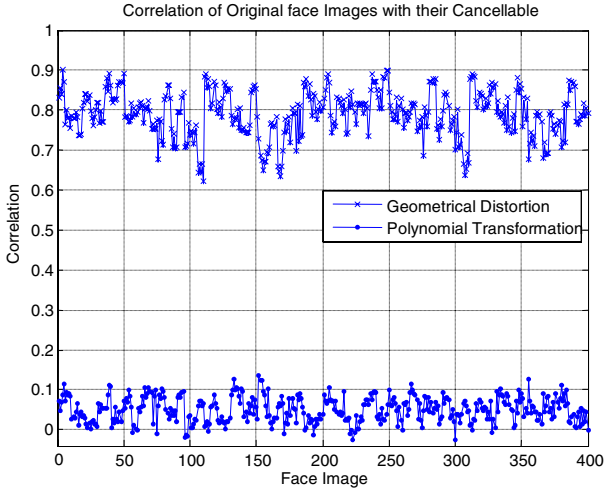

Fig. 5: correlation values between the original image and the cancellable biometric.

This negligible probability indicates the success of a probabilistic polynomial-time algorithm to invert the transformed images, which means very high irreversibility. Fig. 5 presents the correlation values of the all original images with their corresponding cancellable versions. The graph shows very low correlation values for the proposed cancellable data, which should be at the correlation value of 1 in normal cases, this indicates that the images are not related to their original forms. In addition, the polynomial transformation has significantly reduced the correlation between the images themselves, which enhances operation of the PCA that tries to make facial images uncorrelated in order to emphasis the distinctive information for recognition. The unbiased estimator of the variance of the correlation values is 0.0010 with the mean 0.0435 and maximum correlation value of 0.1282. Whereas the morphed [3, 6] cancellable face images have very high correlation with the original data, where the maximum correlation value of the 400 images is 0.9024, mean of 0.7856 and unbiased estimate of the variance of 0.0033. This is due to the retained shape of the face in the distorted images that is not much affected by the transformation. In fig. 6, we present the reversed transformed cancellable biometric of the morphed face image. The images were morphed using a sinusoidal wave that has a variable wavelength parameter along the axes to generate different cancellable version of the face. As observed from the results, the original shape of the face could be approximately achieved when the morphing parameters are available, which reduces the security of the transformed data. However, the proposed cancellable biometric as shown in fig. 4 and argued above does not contain any shape of anything, which makes it impossible to be estimated in a similar fashion.

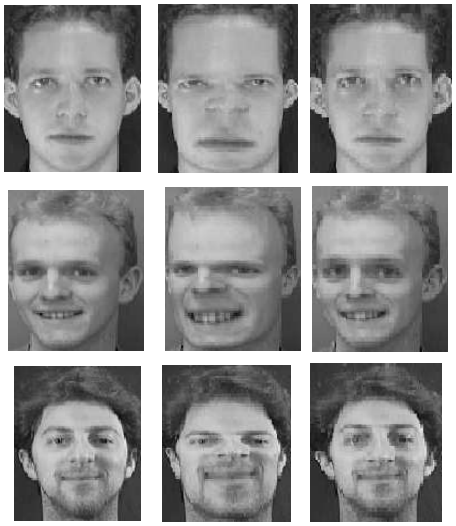

Fig. 6: first column from the left contains the original image from the ORL database, second column contains the morphed images and the last column contains the reversed images.

Fig. 7 shows the recognition accuracy rates of the original biometric data, the proposed cancellable biometric data and the morphed biometric data. The two-dimensional PCA recognition engine has not been changed; the only change was conducted on the input facial images. The recognition rate has been taken up the first 20 principal component vectors with five images for training and five for testing.

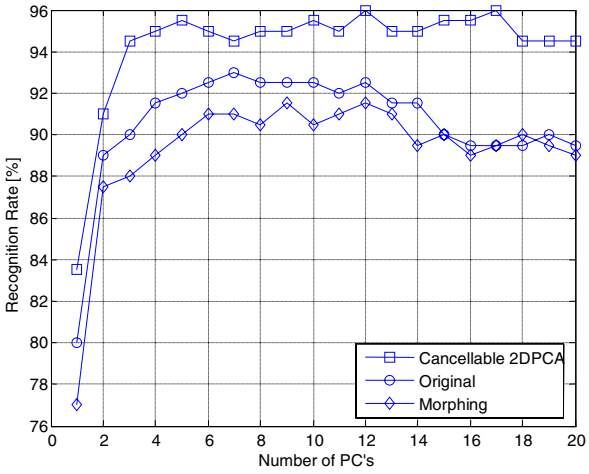

Fig. 7: the recognition accuracy rates up to the 20th PC of the original, morphed and the proposed cancellable biometrics

It show the significant improvement of accuracy rate for the proposed cancellable biometric data over the original and the morphed data, where the highest accuracy for the cancellable data is 96% in comparison with 93% for the original data and 91.5% for the morphed images. This shows that the proposed cancellable method has obtained both security and accuracy of biometric data, whereas the cancellable biometric data is expected to reduce the accuracy rate of the recognition such in the morphed images. The improvement of the recognition accuracy is stated more clearly in fig. 8.

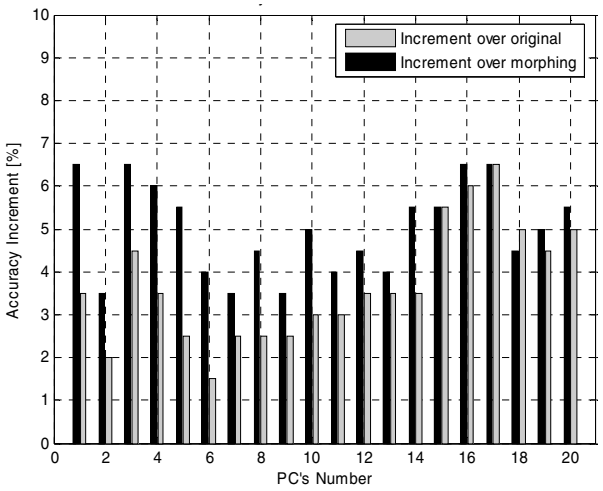

Fig. 8: the improvement of recognition accuracy rates up to the 20th PC for the proposed cancellable biometric over the original and the morphed images.

TABLE 1
ACCURACY OF RECOGNITION AND THE NUMBER OF PRINCIPAL COMPONENT USED FROM DIFFERENT NUMBERS OF TRAINING SAMPLES PER FACE CLASS

Method	Training samples per class									
	1	PC's	2	PC's	3	PC's	4	PC's	5	PC's
Original	75.56%	5	88.13%	4	90.71%	6	91.67%	6	93%	7
Cancellable	77.78%	4	91.56%	9	94.64%	15	94.58	11	96%	12

For the original data, the accuracy improvement has reached the maximum of 6.5% at 17 principal component vectors for recognition, and for the morphed images, the recognition accuracy rate has reach maximum of 6.5% at the 1st, 3rd, 16th and the 17th principal components.

To further examine the method, a comparison between the original and the proposed cancellable biometric is carried out based on the training samples. Table 1 present the top recognition accuracy rates for the first 20 principal components at different number of training samples. As observed, the recognition accuracy of the proposed transformed images is improved for all different samples in the table and the improvement sometimes exceeds 3%, such as 3.93% for the 3 training samples and 3.43% for the 2 training samples. Generally, the number of principal components of the proposed cancellable biometric for recognition is higher. This is due to the nonlinear redistribution of the face image samples that substantially reduces the correlation of each sample. The energy in the cancellable data's covariance matrix that has been normalised by the division of the maximum variance value is more concentrated along the diagonal, where the ratio of the energy average in the matrix (excluding the diagonal) over the energy average in the diagonal is *6.17%*, whereas in the original covariance matrix, the energy is distributed along the diagonal and its surroundings with the ratio of *34.49%*. This means that the covariance of the cancellable data is much more diagonalised than the covariance of the original data. This has contributed to the improvement of the recognition accuracy rate since PCA aims to diagonalised the covariance matrix for good estimated eigenvectors.

IV. CONCLUSION

Biometric authentication cannot replace traditional authentication systems unless biometric data is protected. In this paper, we presented a new and secure biometric recognition for face. The proposed technique operates on the biometric data only. The generated cancellable templates are used for identification in the same way as the original data were used with no changes to the recognition algorithm. If any of these cancellable biometric templates is compromised somehow from the database, a new cancellable biometric can be reissued from the original biometric data without breaching the security of the original biometric. Re-issuance is made available by the modification of the polynomial coefficients. The paper also introduced and analysed the relationship made by the Hadamard between the polynomial transformation and the reconstructed co-occurrence matrix. The mathematical proof shows a new covariance matrix that is emerged using the Hadamard product to generate the final cancellable template. This matrix has linked some distinctive information from both measures which strengthen the accuracy of the recognition performance. Using the 2DPCA algorithm for recognition, with no changes, the accuracy is enhanced to 96% by 3% more than the original biometric data.

ACKNOWLEDGMENT

The authors would like to thank Mr. Risco M. Mutelo for providing the face database, and the 2DPCA recognition implementation.

REFERENCES

[1] R. Chellappa, C. L. Wilson, and S. Sirohey, "Human and machine recognition of faces: a survey," *Proceedings of the IEEE*, vol. 83, pp. 705-741, 1995.

[2] J. Ruiz-del-Solar and P. Navarrete, "Eigenspace-based face recognition: a comparative study of different approaches," *Systems, Man and Cybernetics, Part C, IEEE Transactions on*, vol. 35, pp. 315-325, 2005.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM systems Journal*, vol. 40, pp. 614-634, 2001.

[4] A. B. J. Teoh and D. C. L. Ngo, "Cancellable biometrics featuring with tokenised random number," *Pattern Recognition*, vol. 26, pp. 1454-1460, 2005.

[5] M. Savvides, B. Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proceedings of the 17th International Conference on Pattern Recognition, Vol 3, International Conference on Pattern Recognition*. Los Alamitos: IEEE COMPUTER SOC, 2004, pp. 922-925.

[6] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition*, vol. 35, pp. 2727-2738, 2002.

[7] O. Goldreich, "Chapter 2 - Computational Difficulty," in *Foundations of Cryptography*, 1995.

[8] M. Turk and A. Pentland, "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience*, vol. 3, pp. 71-86, 1991.

[9] J. Yang, D. Zhang, A. F. Frangi, and J.-y. Yang, "Two-dimensional PCA: a new approach to appearance-based face representation and recognition," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 26, pp. 131-137, 2004.

[10] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*: Prentice Hall, 2002.

[11] T. Acharya and A. K. Ray, *Image Processing: Principles and Applications*: John Wiley & Sons, Inc., 2005.

[12] A. Samal, J. R. Brandle, and D. Zhang, "Texture as the basis for individual tree identification," *Information Sciences*, vol. 176, pp. 565-576, 2006.

[13] The Olivetti Research Laboratory and (ORL), "Olivetti database,," in *http://www.cam-orl.co.uk/facedatabase.html*, 1994.