Journal of Korea Multimedia Society Vol. 16, No. 10, October 2013(pp. 1156-1162)
http://dx.doi.org/10.9717/kmms.2013.16.10.1156

A Secure Face Cryptography for Identity Document Based on Distance Measures

Nasim Arshad[†], Kwang-Seok Moon[††], Jong-Nam Kim[†††]

ABSTRACT

Face verification has been widely studied during the past two decades. One of the challenges is the rising concern about the security and privacy of the template database. In this paper, we propose a secure face verification system which generates a unique secure cryptographic key from a face template. The face images are processed to produce face templates or codes to be utilized for the encryption and decryption tasks. The result identity data is encrypted using Advanced Encryption Standard (AES). Distance metric naming hamming distance and Euclidean distance are used for template matching identification process, where template matching is a process used in pattern recognition. The proposed system is tested on the ORL, YALEs, and PKNU face databases, which contain 360, 135, and 54 training images respectively. We employ Principle Component Analysis (PCA) to determine the most discriminating features among face images. The experimental results showed that the proposed distance measure was one the promising best measures with respect to different characteristics of the biometric systems. Using the proposed method we needed to extract fewer images in order to achieve 100% cumulative recognition than using any other tested distance measure.

Key words: Face Cryptography, Encryption, Decryption, Face Recognition, Template Face Image

1. INTRODUCTION

Currently, it is noticed that users tend to choose shorter password as their authentication which can be easily attacked. In recent years, security camera systems have been installed in various public facilities. Biometric technologies such as fingerprint scanning, voice authentication, face recognition, signature, hand geometry and iris recognition is now playing an important role especially in applications related to security issue. A biometric is a unique characteristic of a human body or behavior which will be compared to a stored template to provide authentication of the individual. The Uniqueness of biometrics makes them favourable in many applications requiring a high level of security. Automatic face recognition has apparent advantages over other biometric technologies due to the natural, non-intrusive, and high throughput properties in face data acquisition, hence more intelligent processes are needed to recognize people in image sequences for security camera systems [1]. While fingerprint and iris scan can provide high accuracy rates, they still require complex and specialized scanners. On the contrary, face recognition can be performed with a simple device such as a web-cam, guarantying both a non-intrusive feeling from the scanned person, and a wide range of everyday applications. Over the past three decades,

※ Corresponding Author : Kwang-Seok Moon, Address : (608-737) #2408, A13 Building, Pukyong National University, Daeyon, Nam-gu, Busan, Korea TEL : +82-51-629-6218, FAX : +82-51-629-6259, E-mail : ksmoon@pknu.ac.kr
Receipt date : July 12, 2013, Revision date : Sep. 6, 2013
Approval date : Sep. 9, 2013
[†] Department of Electronics Engineering, Pukyong National University
(E-mail: fs.arshad@gmail.com)
[††] Department of Electronics Engineering, Pukyong National University
[†††] Dept. of IT Convergence & Application Engineering., Pukyong National University
(E-mail: jongnam@pknu.ac.kr)
※ This work was supported by a Research Grant of Pukyong National University (year 2013).

much effort has been made on face recognition using intensity images as input data, although some face recognition systems have good performance under constrained conditions, face recognition is still a great challenge due to variations in illumination, pose, and expression.

Despite the qualities of biometrics, they have a common shortcoming; most of the biometrics-based authentication systems even face authentication systems need a template database, in which a biometric samples and all users' important information are saved.

In this paper, a secure face verification system is proposed. It generates a unique secure cryptographic key from a face template. The face images are processed to produce face templates or code to be utilized for the encryption and decryption tasks. PCA is employed to determine the most discriminating features among face images. Hamming distance and Euclidean distance will be used for the template matching identification process.

The international standard cryptography algorithm-AES has been adopted in our work to produce a high cryptographic strength security protection on the face information. We have chosen AES due to its resistance of the algorithm to cryptanalysis, randomness of the output, computational speed and its efficiency and flexibility on different platform.

2. RELATED WORK

A Number of research works have been reported toward effective combination of biometrics with cryptography. Bodo [2] first proposed to use the data derived from the biometrics templates as the cryptographic key directly in his German patent. Chang et al [3] introduced a method to map the extracted face features to bits, and the bit stream is used as the cryptographic key. A major problem with their methods [2,3] is that the biometrics data is usually subject to drastic variation, and in general cannot produce exactly the same key. Further, neither the biometrics signal nor the key are changeable. If the key is ever compromised, then this biometrics signal is irrevocably lost.

An alternative solution is to randomly generate a cryptographic key, and bind the key with the biometrics features in a way such that neither the biometrics nor the key are revealed even the stored templates are compromised. Juels and Wattenberg [4] proposed a fuzzy commitment scheme to combine the biometrics features with randomly generated keys through a XOR operation. Error correction coding methods are used to tolerance variations of biometrics features. Hao et al [5] implemented a similar scheme in an iris recognition problem. Jeuls et al and Hao et al's methods provides rigorous security, but it is not clear how to produce exactly the same number of bits as the key from face images. Further, the effectiveness of using error correction codes to tolerant large variations, e.g., face images, is yet to be studied.

Ratha et al [6] and Savvides et al [7] are referred to cancellable biometrics, which use one way transformation to convert the biometric signal into irreversible form. Jinyu Zuo, Nalini K. Ratha and Jonathan H. Connell has proposed four cancellable iris biometrics methods conventional iris recognition systems, unwrapped image level or at the binary iris In cancellable biometrics, the system produces a binary yes/no response making it more vulnerable to attacks.

Moi et al [8] implemented an iris biometric cryptography for identity documents. They generate the unique key using the iris template. Wang and Platanaiotis [9] employed a fuzzy vault for face cryptography key generation. In other words a fuzzy vault is utilized for secure binding of randomly generated key with extracted biometrics features.

Sadeghi et al [10] uses a typical scenario for privacy preserving face recognition where a client-server application needs to know whether a specific face image is contained in the database of a

server with the following requirements: the client trusts the server to correctly perform the matching algorithm for the face recognition but without revealing any useful information to the server about the requested image as well as about the outcome of the matching algorithm. The server requires privacy of its database beyond the outcome of the matching algorithm to the client. Nita M. Thakare et al [11] study a through review on biometric standards and Face Image format for data interchange. P.S. Revenkar et al [12] also propose a secure iris authentication by visual cryptography.

As observed from above, most of the previous work and conventional papers, mainly deal on iris cryptography or simple secure face recognition and very few papers have taken the face image for secure cryptography. This is one of the main reasons we're proposing this paper. A secure face cryptography for identity documents will be presented in the next section.

3. PROPOSED METHOD

In this section at first we will describe Karhunen-Loeve transform (KLT)-based face recognition method that is often called principal component analysis (PCA) or eigenfaces. Only the main formulas of this method are presented.

3.1 Image databases

The performance of the PCA based algorithm was evaluated with three image databases, Yale, ORL and Pukyong National University (PKNU). All the three databases consist of 2 categories of images. One category is used for training and the other for the testing purpose. The Yale database consists of 15 different people with nine varying pose, illumination and expressions. It uses 135 images for training and 30 images for testing. The ORL database consists of 40 different people with nine varying pose and expressions. It uses 360 images for training and 40 images for testing. The PKNU database consists of 9 different people with six varying pose and expressions. It uses 54 images for training and 9 images for testing. The training dataset is used for feature extraction procedure and the testing dataset is used for recognition purpose. The varying poses include happy, sad, surprised, angry, wink, big smile expressions. Fig. 1. shows few examples of the test images used in Yale, ORL and PKNU database.

The PCA method has been extensively applied for the task of face recognition [13, 14]. Approximate reconstruction of faces in the ensemble was performed using a weighted combination of eigenvectors (eigenpictures), obtained from that ensemble. The weights that characterize the expansion of the given image in terms of eigenpictures are seen as global facial features.

All the face images in the face database are represented as very long vectors, instead of the usual matrix representation. Because the faces have a similar structure (eye, nose and mouth, position, etc.) the vectors representing them will be corre-

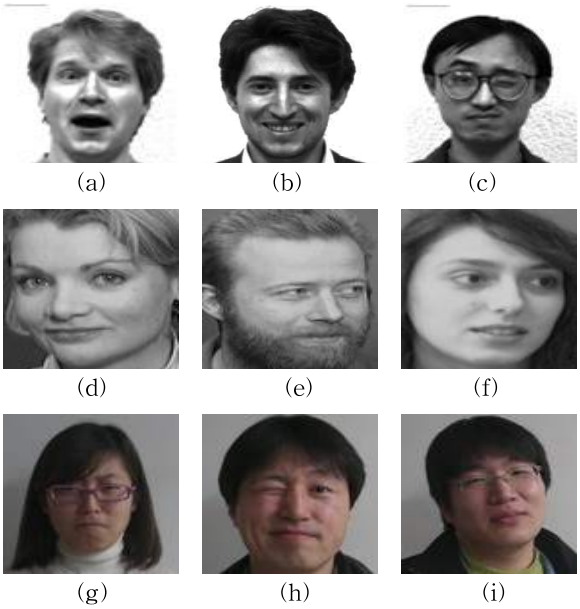


Fig. 1. different expressions and posing: (a, b, c) YALE database showing surprise, happy and blink expressions, (d, e, f) ORL database showing tilted and partial profile face, (g, h, i) PKNU database showing angry, blink and sad expressions.

lated. Hence the face images are represented by a set of eigenvectors developed from a covariance matrix formed by the training of face images. The idea behind eigenimages (or eigenfaces) is to find a lower dimensional space in which shorter vectors will describe face images.

3.2 Computing Eigen Faces

Let Xj be N-element one-dimensional image and suppose that we have r such images (j¼1;...;r). A one-dimensional image-column X from the two-dimensional image (face photography) is formed by scanning all the elements of the two-dimensional image row by row and writing them to the column vector. Then the mean vector, centered data vectors and covariance matrix are calculated:

$$m = \frac{l}{r}\sum_{j}^{r} = {}_1X_j \tag{1}$$

$$d_j = X_j - m \tag{2}$$

$$C = \frac{l}{r}\sum_{j}^{r} = {}_1 d_j d_j^T \tag{3}$$

Here $X = (x_1, x_2, ..., x_N)^T, m(m_1, m_2, ..., m_N)^T, d = (d_1, d_2, ..., d_N)^T$. In order to perform PCA, it is necessary to find eigenvectors. Eigenface technique regards each face image as a feature vector in a high dimensional space by concatenating the rows of the image and using the intensity of each pixel as a single feature. Thus each image can be represented as an n_dimensional random vector x. The found eigen vectors $u = (u_1, u_2, ..., u_N)^T$ are normalized and sorted in decreasing order according to the corresponding eigen values. Later these vectors are transposed and arranged to form the row-vectors of the transformation matrix T. Any data X can be projected onto the eigen space using the following formula:

$$Y = T(X - m) \tag{4}$$

Here $X = (x_1, x_2, ..., x_N)^T$, $Y = (y_1, y_2, ..., y_r, 0, ..., 0)^T$

3.3 Template Matching and Distance Measure

Template Matching is a process used in pattern recognition and also a technique in digital image processing for finding small parts of an image which match a template image. If the template image has strong features, as in our case where the features are the eigen vector, a feature-based approach is considered. Template matching is useful and efficient when working with source of images of large resolution. in order to perform template matching we employ distance measures. Distance metrics are applied for the genuine identification test. The Hamming distance and Euclidean distance or Euclidean metric are the "ordinary" distances between two points that one would measure with a ruler, and is given by the Pythagorean formula. In mathematics, a Euclidean distance matrix is an nxn matrix representing the spacing of a set of n points in Euclidean space. On the other hand Hamming distance is a metric on the vector space of the words of length n, as it fulfills the conditions of non-negativity, identity and symmetry, it can be shown by complete induction that it satisfies the triangle inequality. To compute the distance measures in our algorithm, let X and Y be the eigenfeature vectors of length n. then we can calculate the Hamming distance and the Euclidean distance between these feature vectors as follows:

Hamming distance:

$$d(X, Y) = (X \oplus Y)/2048 \tag{5}$$

where

$\oplus$

is the XOR operation

Euclidean distance:

$$d(X, Y) = L_{p=1}(X, Y) = \| X - Y \| = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{6}$$

Where

X is the eigen-feature vector of face image store

as a template in database. (Training set)

Y is the eigen-feature vector of tested face image. (Testing Set)

3.4 Encryption Process

The face images in the training set are extracted through the face feature extraction process to generate the face template and to produce the face binary code. in this paper the feature extraction process is computing the eigen vectors of the image and perform PCA to generate the face binary code. This binary code for the face image is encrypted with the user identification data using the Advanced Encryption Standards (AES) cryptography. The AES causes the cipher text to be generated, which is later stored in the database.

3.5 Decryption Process

For the decryption process, a tested face image is used. This face image is extracted using face feature extraction to obtain the face template and the face binary code. The eigne computation and PCA algorithm are applied to the test image to generate the test face binary code. The binary code templates from the training set and from the testing set are matched using the two distance metrics. If both distance measures produce a matching template in the stored database, the decryption process will begin else the system will stop in other words the test face is not identified. The decryption process is the reverse of the encryption process. That is the matched template will employ the AES cryptography along with the cipher text to obtain the user identification data.

4. EXPERIMENTAL RESULTS

The proposed algorithm was executed on an Intel E2200 @ 2.20GHz CPU, with 3 GB RAM. All our algorithms were implemented using MATLAB programming software. Fig. 2. shows the overall

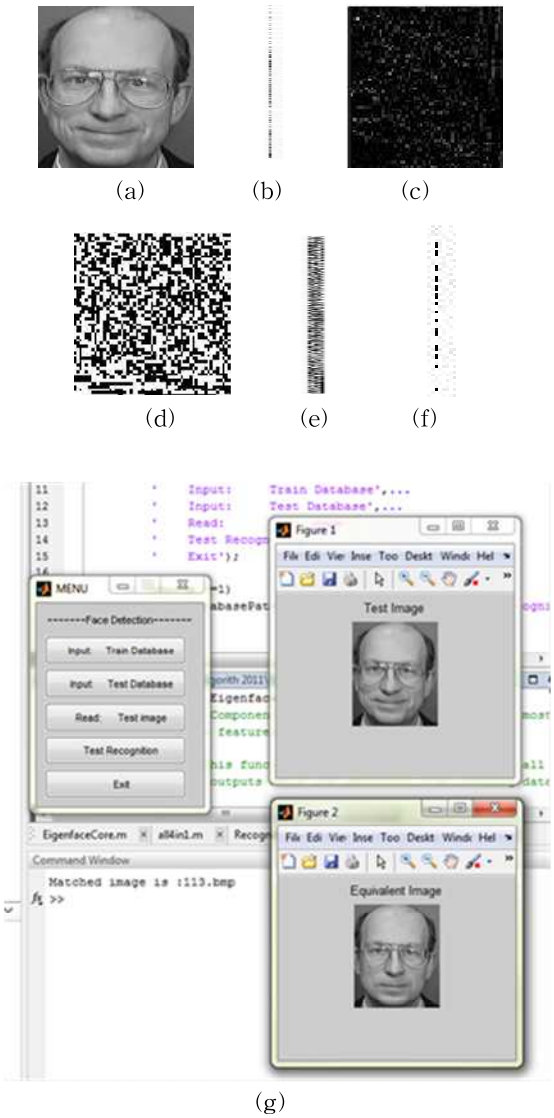


Fig. 2. Overall implementation of the program: (a) original test image for id, (b): reshaping 2D image to 1D vector, (c) eigen face code, (d) eigen vectors, (e) projection of all images in training set, (f) the projected test image for identification, (g) identified the person based on distance measures.

algorithm procedure for one test image taken from ORL dataset. Table 1, shows the results of the proposed algorithm for the 3 different databases used. The results reveal that the proposed algorithm is not affected by the shadows, expressions, illuminations or the background of the object. The overall recognition rate for the test images was 95.27%.

Considering more number of eigenvectors results in increased recognition rates. But also, it in-

Table 1. Experimental Results

Dataset	dimensions	No. of images in train-set	No. of images in test-set	recognition rate %
Yale	100*100	135	30	93.33
ORL	100*100	360	40	92.5
PKNU	100*100	54	9	100

creases the computational cost which grows linearly with the number of eigenvectors.

The complexity of the above method is a bit high. This is due to the encryption and decryption process. In other words encryption should be employed for all the images stored in the training set.

5. CONCLUSION

In this paper, a secure face verification system is proposed. It generates a unique secure cryptographic key from a face template. The face images are processed to produce face templates or code to be utilized for the encryption and decryption tasks. PCA is employed to determine the most discriminating features among face images. Hamming distance and Euclidean distance will be used for the template matching identification process. The experiments showed that the proposed distance measure could be among one of the best measures with respect to different characteristics of the biometric systems. Using the proposed algorithm we achieve a detection rate of overall 95.27%.

REFERENCES

[1] Ch. H. Lee, "Definition of Optimal Face Region for Face Recognition with Phase-Only Correlation," *KISPS*, Vol. 13, No. 3, pp. 150-155, 2012.

[2] A. Bodo, "Method for Producing a Digital Signature with Aid of a Biometric Feature," German Patent DE 42 43 908 A1, 1994.

[3] Y.J. Chang, W. Zhang, and T. Chen, "Biometrics-based Cryptographic Key Generation," *Proc. of IEEE Int. Conf. on Multimedia and Expo,* pp. 2203-2206, 2004.

[4] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," *Proc. of sixth ACM Conf. on Computer and Communication Security*, pp. 28-36, 1999.

[5] F. Hao, R. Anderson, and J. Daugman, "Combining Crypto with Biometric Effectively," *IEEE Trans. on Computers*, Vol. 55, No. 9, pp. 1081-1088, 2006.

[6] K.N Ratha, S. Chikkerur, J.H. Connel, and R.M. Bolle, "Generating Cancellable Fingerprints,"N *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, pp. 561-572, 2007.

[7] M. Savvides, B.V. Kumar, and P. Khosla, "Cancellable Biometric Filters for Face Recognition," *Proc. the 17th International Conferenceon Pattern Recognition*, Vol. 3, pp. 922-925, 2004.

[8] S.H. Moi, N.B. Rahim, P. Saad, P. Sim, Z. Zakaria, and S. Ibrahim, "Iris Biometric Cryptography for identity Document," *International Conference on Soft Computing and Pattern Recognition*, pp. 736-741, 2009.

[9] Y. Wang and K.N. Plataniotis, "Fuzzy Vault for Face Based Cryptographic Key Generation," *Biometric Symposium*, 2007.

[10] A. Sadeghi, T. Schneider, and I. Wehrenberg, "Efficient Privacy-Preserving Face Recognition," *ICISC,* pp. 229-224, 2009.

[11] M.T. Nita and V.M. Thakare, "Biometrics Standards and Face Image Format for Data Interchange-Review," *Int Journal of Advan-*

ces in Engineering & Technology, Vol. 2. pp. 385-392, 2012.

[12] P.S. Revenkar, A. Anjum, and W.Z. Gandhare, "Secure Iris Authentication using Visual Cryptography," *Int Journal of Computer Science and Information Security*, Vol. 7, No. 3, pp. 218-221, 2010.

[13] J.J. Park and K.M. Kim, "Face Recognition using Eigenface," *KISPS*, Vol. 2, No. 2, pp. 1-6, 2001.

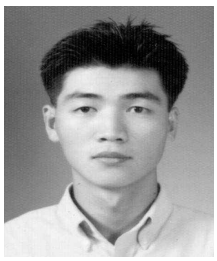
[13] W. O. Lee, Y. H. Park, E. C. Lee, H. K. Lee and K.R. Park, "Tracking and Face Recognition of Multiple People Based on GMM, LKT and PCA," *Journal of Korea Multimedia Society*, Vol. 15, pp. 449-471, 2012.

Nasim Arshad

2005 Mysore University, India Computer Science (B.Sc)
2007 Mysore University, India Computer Science (M.Sc)
2009~present Pukyong National University, South Korea (PhD student)
Research Interest: Pattern Recognition, Image/Video Processing and Compression, VLSI design for real-time Video Applications

Kwang-Seok Moon

1979 Kyungpuk National University, Korea Electronic Engineering(B.Sc)
1981 Kyungpuk National University, Korea Electronic Engineering(M.Sc)
1989 Kyungpuk National University, Korea Electronic Engineering(PhD)
1990~present Pukyong National University, Korea, Electronic Engineering (Professor)
Research Interest: Video/Signal Processing, Adaptive Signal Processing



Jong-Nam Kim

1995 University of Science and Technology, Electronic Engineering (B.Sc)
1997 Gwangju Institute of Science and Technology, Korea (M.Sc)
2001 Gwangju Institute of Science and Technology, Korea (PhD)
2004~present Pukyong National University, Korea, IT convergence and Tele-communication Engineering (Professor)
Research Interest: Pattern Recognition, Image/Video Processing and Compression, VLSI design for real-time Video Applications