IOSR Journal of Electronics & Communication Engineering (IOSR-JECE)
ISSN(e) : 2278-1684 ISSN(p) : 2320-334X, PP 14-19
www.iosrjournals.org

A data securing approach for face images in biometric database

Aswathy Elma Aby[1], K.Vijayakumar[2]

[1] Department of Electronics and Communication, Toc H Institute of Science and Technology, India
[2] Department of Electronics and Communication, Toc H Institute of Science and Technology, India

ABSTRACT : *Biometrics refers to statistically analyzing biological characteristics of a person for authentication as well as identification and is of prime importance because of the eminent role security plays in different areas in day to day life. Application of such system includes terrorist determination, passport control, banking etc. All in all, biometrics is not a secure approach unless; suitable countermeasures are employed to make the enrolled data inaccessible to intruder. This work introduces a technique for providing biometric face data secure by using Grey level Extended Visual Cryptography (GEVCS), Principal Component Analysis (PCA) and Euclidian distance approach. The performance is analyzed using Peak Signal to Noise Ratio (PSNR). The results show that the reconstructed image as well as the share images is similar in appearance to the original target image and the host images respectively.*

Keywords - *Biometric database, Euclidian distance, GEVCS, PCA, PSNR*

1. Introduction

Biometrics refers to identifying human features for personal authentication. Multimodal biometric approaches which provides multiple evidences of the same identity is preferred over unimodal biometrics due to its design limitations such as noise in input data, intra-class variation, interoperability, vulnerability against spoof attacks, inter-class similarities etc. To make the data inaccessible for imposter, some countermeasures are also to be employed (e.g. encryption or anonymous techniques). Unless storing biometric features in a server will not be secure.

For protecting the privacy of biometric data enrolled in a database, Davida et al. [1] and Ratha et al. [2] proposed a technique to store in the database, the transformed biometric template instead of the original biometric template. A three-step hybrid approach is proposed by Feng et al. [3] that combined the advantages of cancelable biometrics and cryptosystems. Other than these methods, researchers suggest various image hiding approaches [4]–[6] to provide anonymity to the stored biometric data. A face swapping technique which protects the identity of a face image by automatically substituting it with replacements taken from face images of a public dataset is proposed by Bitouk et al [7]. However, in the case of face swapping and aggressive de-identification, there are chances of original face image to be lost.

Naor and Shamir [8] introduced a secure way to allow secret sharing of images without any cryptographic schemes called visual cryptography scheme (VCS). In this scheme, encryption is performed such that decryption can be done using the human visual system. Later, Nakajima and Yamaguchi [9] presented a 2-out-of-2 extended VCS known as the gray-level extended visual cryptography scheme (GEVCS) for natural image encoding. Recently, Arun Ross and Asem Othman [10] explored the possibility of using GEVCS for imparting privacy to biometric face images using Active Appearance Model (AAM) [11].

A biometric data hiding technique which addresses template protection requirements such as diversity, revocability, security and better recovery performance along with reduced computational complexity and easier decryption is preferable. This work explores the possibility of using GEVCS along with Principal Component Analysis (PCA) and Euclidean distance method to satisfy these requirements. Privacy to biometric face image is ensured by decomposing the original image into two images such that the original image can be recovered only when both images are simultaneously available. Also, any information about the original image cannot be revealed by individual component images. It provides successful matching of face images reconstructed from the sheets and also less cross-database matching for determining identities.

Biometric processing includes enrollment and authentication/identification. The private biometric data is sent to a trusted third party after enrollment. Once the trusted entity receives the data, the image is then decomposed into two images known as sheets. The decomposed components are then transmitted and stored in two different database servers. It thus prevents revealing the identity of private data to either server. During the authentication process, upon the request of the trusted entity to each server, the corresponding sheets are transmitted to it. In order to reconstruct the private image, sheets are overlaid (i.e., superimposed).

After decomposing, each private face image is encrypted into two different public host face images. While using non-face images as hosts, it may result in visually revealing the existence of a secret face. Decomposing the face image into random noise structures may also pique the interest of an eavesdropper by suggesting the existence of secret data.

The rest of the paper is organized as follows. Section II gives an idea about the Visual Cryptographic technique and section III explains the proposed approach for securing private face images. Section IV shows the experimental results, section V concludes the paper and section VI proposes the future scope of the work.

2. Visual Cryptography

2.1 Visual Cryptography Scheme (VCS)

The visual cryptography scheme (VCS), introduced by Naor and Shamir [8] provides a simple and secure way to allow the secret sharing of images without any cryptographic computations. The basic scheme is referred to as the k-out-of-n VCS. It is also denoted as (k, n) VCS [8] and it deals with binary images. In this scheme, an original binary image T is encrypted in 'n' images, such that

$$T = S_{h_1} \oplus S_{h_2} \oplus S_{h_3} \oplus \cdots \oplus S_{h_k} \qquad (1)$$

where $\oplus$ is a Boolean operation, $k \leq n$, 'n' is the number of noisy images, S_{hi}; $h_i \in (1,2,\ldots,k)$, is a share image, and it appear as white noise. Using individual S_{hi}'s, it is difficult to decrypt the secret image T [8]. The encryption is done such that 'k' or more out of 'n' generated images are necessary to reconstruct the original private image T.

2.2 Gray-Level Extended Visual Cryptography Scheme (GEVCS)

In VCS, the sheets appear as a random set of pixels. They may generate curiosity of an interceptor by suggesting the existence of a secret image inside. To mitigate this problem, Naor and Shamir [8] suggested an approach to reformulate the sheets as natural images. Such a framework was introduced by Ateniese et al. [12] known as the extended VCS. A theoretical framework to apply extended visual cryptography on grayscale images (GEVCS) is proposed by Nakajima and Yamaguchi [9]. They also introduced a method to enhance the contrast of the target images in it. For GEVCS, the dynamic range of the original and host images are at first changed, gray-level images are transformed into meaningful binary images (also known as halftoned images) and then a Boolean operation is applied on the halftoned pixels of the two hosts and the original image.

During encryption, the sub pixel arrangement in the shares of both hosts has to be controlled to obtain required transparency (the number of white sub pixels) of the target pixel. But there are cases when the required transparency for the corresponding pixel in the target image cannot be obtained, however the shared sub pixels are rearranged.

Nakajima and Yamaguchi [9] described a method to decrease the number of violated triplets by performing an adaptive dynamic range compression and thereby enhance the image quality (contrast). The error

generated while adjusting the gray levels of the conflicting triplets are diffused to the nearby pixels. Thus to facilitate this adjustment, both halftoning and encryption are done simultaneously.

3. Securing Face Images in Database

Let H be the desired private face image and R={P_1, P2 … P_N} the public dataset containing a set of host images. At first two host images P_i and P_j, i≠j and i,j =1,2…N are to be selected from R that can hide the private face image. Variations in face geometry and texture between the private face image and the images in the public dataset may result in perceptibility of the impact of the target image on the sheet images and vice versa. By carefully choosing host images for a particular private image, this issue can be mitigated. The steps for this will be explained in more detail in the following subsections.

A. Principal component analysis (PCA)

Host images are to be selected such that they are most likely to be compatible with the private image. For this we here used principal component analysis with "Eigenface" [13] approach due to its simplicity, speed and learning capability. To determine the similarity between private face image and candidate host images, the design of the face recognition system is based upon "eigenfaces". By means of PCA the features of the original images of the training set are transformed into a set of eigenfaces E. For each image of the training set, the weights are calculated and are stored in a set W. Upon observing an unknown image Y, the weights for that particular image is calculated and stored in the vector W_Y. For host selection, W_Y is compared with the weights of images of the training set W.

B. Selection of Hosts

Selection of hosts is done by determining the distance 'd' between W_X , the weight of unknown image X and weights of images of the training set W. The most common approach is the Euclidean distance, but other measures may also be used. This work presents the results for the Euclidean distance comparison [14]. If A and B are two vectors of length D, the distance between them is determined as follows:

$$\text{Euclidean distance: } d(A, B) = \sqrt{\sum_{i=1}^{D}(ai - hi)^2} = \|A\text{-}B\| \qquad (2)$$

The distances are then sorted in order to locate two host images, H_{S1} and H_{S2}, which are most likely to be compatible with the secret image for encryption.

C. Secret Encryption and Reconstruction

To encrypt the secret image H in the two host images P_{S1} and P_{S2}, GEVCS is used. It generates two data encrypted sheet images denoted as S_1 and S_2, respectively. In order to reveal the secret private image, S_1 and S_2 are superimposed. While reconstructing the final target image, to retain the original image size, pixel expansion step is reversed.

4. Experimental Results

We used MATLAB simulation to evaluate the performance of proposed technique. First we assigned a public dataset containing a set of candidate host images that can hide the assigned private face image. Fig.1 shows the assigned public dataset for host selection. For the analysis, we took a dataset consisting of images of four persons with three images each.

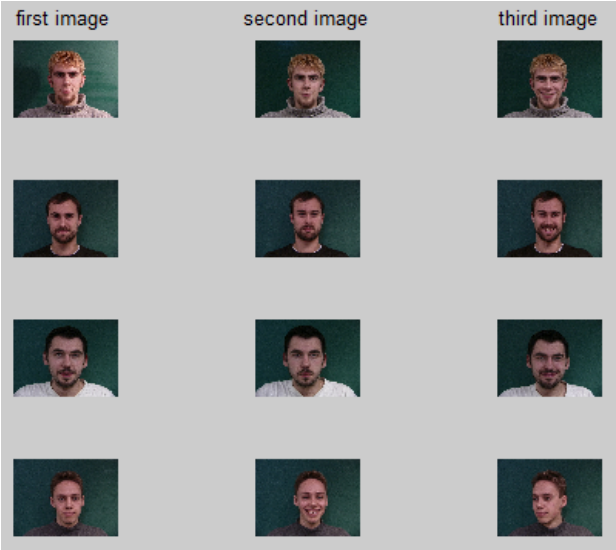

Fig.1 Public dataset

The first task is to train the images of each person in the dataset to generate corresponding eigenface. It is done using PCA. Fig. 2 and fig.3 shows an example of the dataset images of a person and the corresponding eigenface respectively.

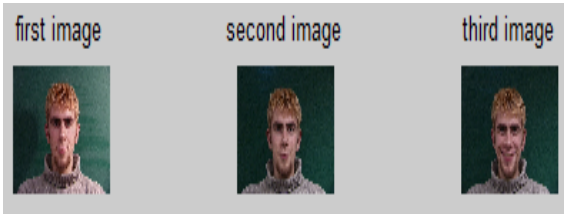

Fig.2 Dataset images of a person

Fig.3 Eigenface

Selection of two host images from the public dataset to encrypt the private face image is done by analyzing these eigenfaces. The images are selected such that, they are most likely to be compatible with the private face image. Face images which have minimum Euclidian distance with the private face image are selected as host images. Fig.4 shows the process of host selection.

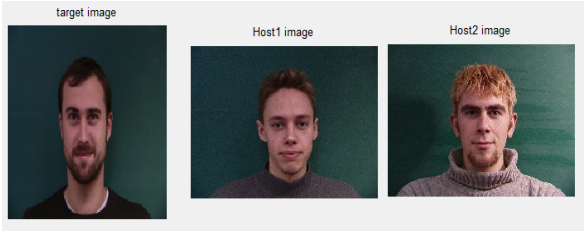

Fig.4 Host selection

The private face is then encrypted in selected host images, halftoned and is stored in two different database servers. The halftoned private face image which is then encrypted in host images is shown in fig.5. The

reverse processes are performed during the decryption. Fig.6 shows the encrypted share images stored in database and the recovered private face from them.

Fig.5 Private image before encryption

Fig.6 Share images and the recovered private face image

The Peak Signal to Noise Ratio (PSNR) is used to analyze the matching performance of the original as well as the reconstructed probes.

$$PSNR = 10 \log_{10} [255^2 / MSE] \quad (3)$$

$$\text{Mean Square Error, MSE} = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{1}{mn} (xij - yij)^2 \quad (4)$$

where x_{ij} & y_{ij} denotes corresponding pixel values of original & reconstructed image respectively and *m* & *n* denotes number of rows and columns of each image matrix.

The reconstructed image as well as the share images is similar in appearance to the original target image and the host images respectively. Thus it prevents the intruders not to have any idea of the existence of a secret face image to be encrypted in the share images. Performance analysis of reconstructed image gives an appreciable PSNR value which shows the better recovery performance of proposed approach.

5. Conclusion

This work explored the possibility of using GEVCS and PCA for imparting privacy to biometric templates. To protect the privacy of a face image in the database, the input private face image is decomposed and encrypted in two independent host images such that the private face image can be reconstructed only when both sheets are simultaneously available. We were able to obtain the reconstructed images from the sheet images similar to original private image. Cross-matching across applications to reveal the identity of a private face image will be difficult since different applications can adopt different sets of host images for encrypting the same private face image. Also it is computationally hard to obtain the private biometric image from the individual stored sheets due to visual cryptography, which enhance the system security. By using distributed servers to store the sheets, the security of the original private image can be further maximized.

REFERENCES

[1] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Security and Privacy*, 1998, pp. 148–157.

[2] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[3] Y. Feng, P. Yuen, and A. Jain, "A hybrid approach for face template protection," in *Proc. SPIE Conf. Biometric Technology for Human Identification*, Orlando, FL, 2008, vol. 6944.

[4] A. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[5] J. Dong and T. Tan, "Effects of watermarking on iris recognition performance," in *Proc. 10th Int. Conf. Control, Automation, Robotics and Vision,2008 (ICARCV 2008)*, 2008, pp. 1156-1161.

[6] N. Agrawal and M. Savvides, "Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching," in *Proc. Computer Vision and Pattern Recognition Workshop*, 2009, vol. 0, pp. 85–92.

[7] D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "Face swapping: Automatically replacing faces in photographs," *ACMTrans. Graph.*, vol. 27, no. 3, pp. 1–8, 2008.

[8] M. Naor and A. Shamir, "Visual cryptography," in *Proc. EUROCRYPT*, 1994, pp. 1–12.

[9] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," *J. WSCG*, vol. 10, no. 2, pp. 303–310, 2002.

[10] Arun Ross and Asem Othman, "Visual Cryptography For Biometric Privacy," in IEEE Transactions On Information Forensics And Security, Vol. 6, No. 1, March 2011

[11] T. Cootes *et al.*, "Active appearance models," *IEEE Trans. PatternAnal. Mach. Intell.*, vol. 23, no. 6, pp. 681–685, Jun. 2001.

[12] G. Ateniese, C. Blundo, A. Santis, and D. Stinson, "Extended capabilities for visual cryptography," *Theor. Comput. Sci.*, vol. 250, no. 1–2, pp. 143–161, 2001.

[13] Mamta Dhanda, "Face recognition using eigenvectors from Principal component analysis" in International Journal of Advanced Engineering Research and Studies/ Vol. I/ Issue II/January-March, 2012/37-39

[14] Marijeta Slavković, Dubravka Jevtić, "Face Recognition Using Eigenface Approach", Serbian Journal Of Electrical Engineering, Vol. 9, No. 1, February 2012, 121-130