ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Framework for Preservation of Biometric Information with Facial Template Protection using Gray-Level Extended Visual Cryptography Scheme

Dhara Kumari
M.Tech Scholar
SRCEM College
Palwal (India)

Dr. Dinesh Kumar
HOD Dept. of CSE
SRCEM College
Palwal (India)

Dr. Rajni Sharma
Assistant Professor (Computer Science)
PT.J.L.N. Govt P.G College
Faridabad (India)

Abstract: The main idea of this paper is to explore the privacy of information security and network security during the transmission of data using the Visual Cryptography (VC) techniques onto the area of authentication using Biometrics data (face images). A face image is usually registered in a central database as an important piece of personal information. To protect the copyright and privacy of face images, we propose a visual cryptography for transmission of any type of information privacy to biometric data (face images, iris codes, fingerprint images etc). In which we suggest an approach to protect the privacy of a specific face data set (known as a private face images) by encrypting its face images using face images from another set (known as a public face images). Each private face image will be encrypted by using two host images from the public face images via the GEVCS method based on the XOR and OR operation. . In this work, private face image is dithered into two host face images (known as sheets) that are stored in two separate database servers(XM2VTS and IMM) such that the private image can be revealed only when both sheets are simultaneously available; at the same time, the individual sheet images do not reveal the identity of the private image. Experimental results show the proposed scheme not only to protect the privacy of face images in database, but also shows better robustness to noise, filter, JPEG compression, rotation and other attacks.

Keywords: Visual Cryptography, Biometric Data, Private Face, Public Face, GEVCS, XM2VTS, IMM, Privacy, OR operator.

I INTRODUCTION

Biometric deal with recognizing a person or verifying the identity of a person based on physiological or behavioral characteristics such as face, iris, gait, voice and fingerprints. Biometric authentication has been widely used for a access control and security systems over the past few years, face recognition has become one of the most active and challenging research topics in pattern recognition and computer vision fields due to its wide range of applications in biometrics, human-computer interaction, information security and so on [1], [2]. Although many researchers have proposed various algorithms for face recognition [1], [2], it is still a challenging problem [3], [4]. The purpose of and the driver of further research in the area of face recognition are security applications and human-computer interaction that represents an intuitive and non-intrusive method of recognizing people.

In this research paper, we explore the security of digital biometric information like face images that stored in a central database has important piece of personal information. A biometric authentication system operates by acquiring raw biometric information (e.g., face image), extracting a feature set from the data (e.g., Eigen-coefficients), and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity. During enrollment, the template of a person in the database is generated and is often stored along with the original raw data. In some situation, this data may have to be transmitted across a network. Thus, the security of transmitted data has heightened the need to accord privacy[1] to the information by sufficiently protecting the contents of the database.

II LITERATURE SURVEY

While developing our research paper, we have gone through lot of reviews and got various feedbacks and suggestions from various ways. To protect the privacy of an individual enrolled in a biometric database, Davida *et al.* [5] and Ratha *et al.* [6] introduced storing a transformed biometric template instead of the original biometric template in the database. This term referred to as a private template [5] or a cancelable biometric [6].

Feng *et al.* [7] introduced a three-step hybrid approach that combined the advantages of cryptosystems and cancelable biometrics. Apart from these methods, various image hiding approaches [8]–[10] have been suggested by researchers to provide anonymity to the stored biometric data.

Newton *et al.* [11] and Gross *et al.* [12] proposed a face de-identification algorithm that minimized the chances of

performing automatic face recognition while preserving details of the face such as expression, gender, and age for privacy to face images present in surveillance videos.

Bitouk *et al.* [13] proposed a face swapping technique which protected the identity of a face image by automatically substituting it with replacements taken from a large library of public face images. However, in the case of face swapping and aggressive de-identification, the original face image can be lost. Recently, Moskovich and Osadchy [14] proposed a method to perform secure face identification by representing a private face image with indexed facial components extracted from a public face database.

III .WORKING NATURE OF THIS PROPOSED SYSTEM

In this research paper, we suggest an approach (visual cryptography) to protect the privacy of biometric information (viz., raw images) by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available; further, the individual component images do not reveal any information about the original image. Figure 1 show block diagram of the proposed approach for biometric modalities (like face images).

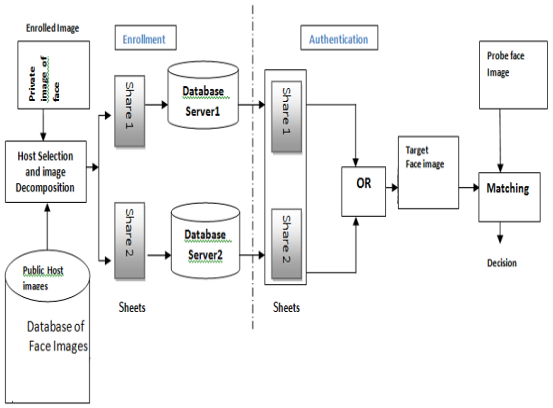

Fig. 1 Proposed approach for de-identifying and storing a face image.

[1]The term "privacy" as used in this paper refers to the de-identification and security of biometric data.

In this figure there are two possibilities will be generated:

- Enrollment Phase
- Authentication Phase.

Enrollment Phase: In this case, the private biometric data is sent to a trusted third-party entity. Once the trusted entity receives it, the biometric data is decomposed into two images and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server. Figure 2 shows block diagram of the Enrollment Phase.

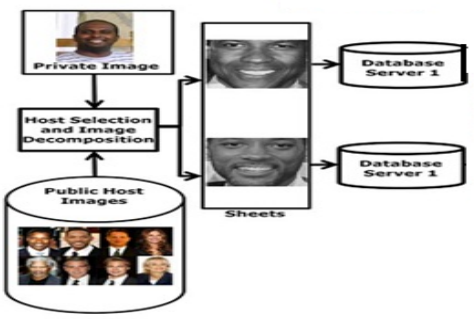

Fig. 2 Process of Enrollment Phase

Authentication Phase: In this case, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are overlaid (i.e., superimposed) in order to reconstruct the private image thereby avoiding any complicated decryption and decoding computations that are used in watermarking [8], [9], steganography [10], or cryptosystem [15] approaches. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image. Figure 3 shows block diagram of the Authentication Phase.

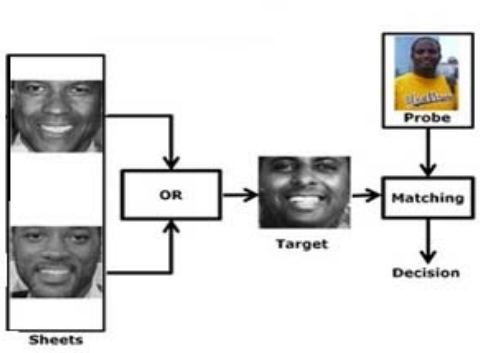

Fig. 3 Process of Authentication Phases

In Figure 2, each private face image is decomposed into two independent public host images. In this scenario, the private image can be viewed as being encrypted into two host face images. The use of face images as hosts for a private face image (as opposed to using random noise or other natural images) has several benefits in the context of biometric applications:

1. The demographic attributes of the private face images such as age, gender, ethnicity, etc. can be retained in the host images thereby preserving the demographic aspects of the face while perturbing its identity. Alternately, these demographic attributes, as manifested in an individual's face, can also be deliberately distorted by selecting host images with opposite attributes as that of the private image.
2. A set of public face images (e.g., those of celebrities) may be used to host the private face database. In essence, a small set of public images

can be used to encrypt the entire set of private face images.

3. Using non face images as hosts may result in visually revealing the existence of a secret face as can be seen in Figure. 4.

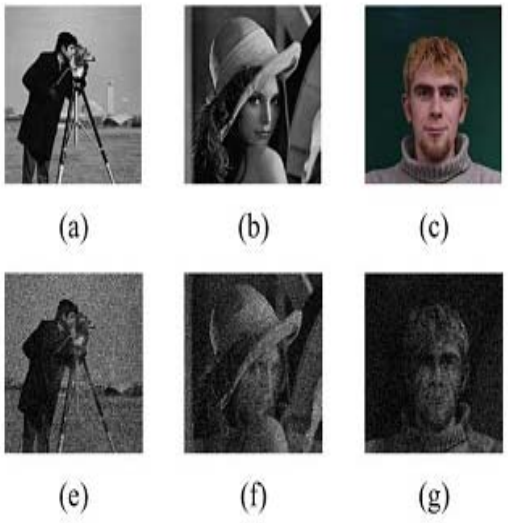

Fig. 4 Encryption of a private face image in two standard host images.

In Figure 4, Encryption of a private face image in two standard host images using the attribute of private face image as a:

- (a) Host 1: Cameraman image.
- (b) Host 2: Lena image.
- (c) A private face image.
- (e) and (f) The two host images after visual encryption (two Sheets).
- (f) Result of superimposing (e) and (f).

Finally, while decomposing the face image into random noise structures may be preferable, it can pique the interest of an eavesdropper by suggesting the existence of secret data.

The rest of the paper is organized as follows. In Section IV a basic introduction to visual cryptography and its extensions are presented. Sections V discuss the proposed approach for securing face images and future scope. Section VI concludes the paper.

IV VISUAL CRYPTOGRAPHY

Privacy protection is very important in today's world where personal information, images are generally shared to each other through the network. When we are sharing information on internet number of outsiders or intruder try to hack it before the information is received by the receiver. So, to protect the information from hackers visual cryptography scheme(VCS) is used that was introduce by [16] Moni Naor and Adi Shamir in 1994 which allows visual information like pictures, text, data to be encrypted in such a way that decryption becomes a very easy operation that does not require any type of computation or computer. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. The VCS describes the way in which an image is encrypted and decrypted.

- There is the k-out-of-n scheme that says n shares will be produced to encrypt an image, and k shares must be stacked to decrypt the image [17]. If the number of shares stacked is less than k, the original image is not revealed.
- In the 2-out-of-n scheme n shares will be produced to encrypt an image, and any two shares must be stacked to decrypt the image.
- In the n-out-of-n scheme, n shares will be produced to encrypt an image, and n shares must be stacked to decrypt the image. If the number of shares stacked is less than n, the original image is not revealed. Increasing the number of shares or participants will automatically increase the level of security of the encrypted message. This scheme work on Two-out-of-Two Scheme (2 subpixels layer) and Two-out-of-Two Scheme (4 subpixels layer) using the "OR" and "XOR" operation.

For example, explanation of Two-out-of-Two Scheme (4 subpixels layer):

In order to explain the 2-out-of-2 VCS with 4-subpixel layout each pixel is expanded into 2×2 subpixels as shown in Figure 5.

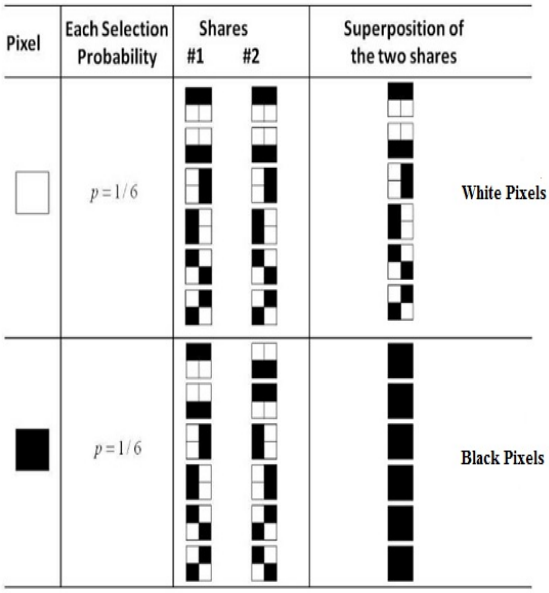

Fig. 5 Partitions for black and white pixels for 2-out-of-2 scheme (4 subpixels)

In fig. 5, one pixel of the original image corresponds to four pixels in each share. Therefore, six patterns of shares are possible. For the 2-out-of-2 VCS with 4-subpixels, the basis matrices S0 and S1 are designed by using fig. 5 as follows:

$$S^0 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$S^1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

The relative difference α and contrast β for the above basis matrices are computed as: α = ½ β = 2. Let C^0 and C^1 be:

$$C_0 = \{ \pi \left(\begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix} \right) \}$$

$$C_1 = \{ \pi \left(\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \right) \}$$

To analyze the security of the *2-out-of-2* with 4-subpixel layout VCS, the dealer randomly chooses one of the pixel patterns (black or white) from the fig. 5 for the shares S1 and S2. The pixel selection is random and the shares S1 and S2 consist of equal number of black and white pixels. Therefore, by inspecting a single share, one cannot identify whether the secret pixel is black or white. Thus, this method provides perfect security. The two participants can recover the secret pixel by superimposing the two shared subpixels. If the superimposition results in four black subpixels, the original pixel was black; if the superimposition creates two black and two white subpixels, it indicates that the original pixel was white.

In 2002, Nakajima and Yamaguchi [18] presented a 2-out-of-2 extended VCS for natural images. They suggested a theoretical framework to apply extended visual cryptography on grayscale images (GEVCS) and also introduced a method to enhance the contrast of the target images. Figure 4 show as encoding a natural image in innocuous images using (GEVCS). In this work, the extended VCS for grayscale images are used to secure face images.

Gray-Level Extended Visual Cryptography Scheme (GEVCS)

Gray scale cryptography scheme (GEVCS) is the extended version of visual cryptography. This scheme operates by changing the dynamic range of the original and host images, transforming the gray-level images into meaningful binary images (also known as halftoned images) and then applying a Boolean operation on the halftoned pixels of the two hosts and the original image. The gray scale cryptography is dividing into 3 steps:

- The first step is halftone image and partitioning the halftone image.
- In the second step**,** the number of black pixels in each cluster from the halftone image are counted and saved in a template.
- The third step starts from the first block in the top left.

V SECURING PRIVATE FACE IMAGES

Let P= {H1, H2, H3,……,Hn} be the public dataset containing a set of candidate host images that can hide the assigned private face image O. The first task is to select two host images Hi and Hj, i≠j and i, j=1,2,2,……,N from P. Note that due to variations in face geometry and texture between the images in the public dataset and the private face image, the impact of the target image on the sheet images and vice versa may become perceptible. This issue can be mitigated if the host images for a particular private image are carefully chosen. Figure 6 shows the block diagram that illustrates the key steps of the proposed approach.

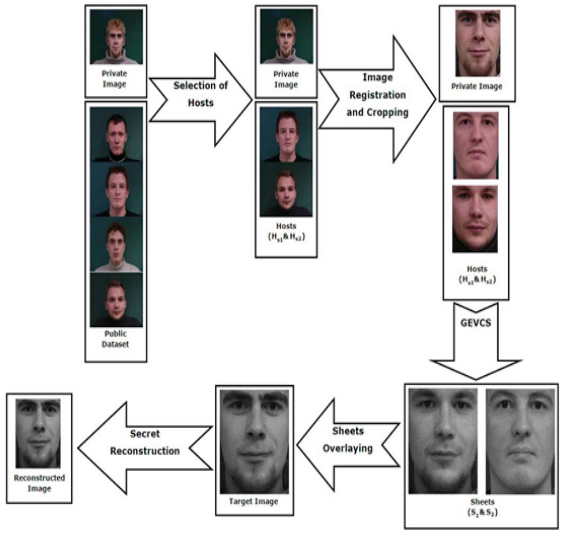

Fig. 6 Block diagram of the proposed approach for storing and matching face images.

Scope for securing private face images:

- This project at start should aim at the security of the private face images.
- Only qualified subset of shares can recover the secret image.
- Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image. All the shares are meaningful images.
- The authentication must be valid for the face image registered before. It can be used at all security related institutions like military, offices, confidential laboratories.

VI CONCLUSION AND DISCUSSION

This paper includes a methodology to protect the privacy of a face database by decomposing an input private face image into two independent sheet images such that the private face image can be reconstructed only when both sheets are simultaneously available. The proposed algorithm selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. Increasing the pixel expansion factor can lead to an increase in the storage requirements for the sheets. In the recent literature there have been some efforts to develop a VCS without pixel expansion. But no such scheme currently exists for generating sheets that are not random noisy

images. Thus, more work is necessary to handle this problem. Future work can be achieved by using 2-out-of-2 VCS with 4-subpixel layout using the Extended Gray-level Visual Cryptography Scheme (EGVCS) that is based on the XOR and XNOR operation in which we combine two biometric information (face and fingerprint templates) for privacy and protecting the all type of information during the transmission of data over the Internet. It also works on the central database for biometric information (like face, fingerprints, and iris).

VII REFERENCES

[1]. Li SZ, Jain AK (2011) Handbook of face recognition, Springer.

[2]. Jafri R, Arabnia HR (2009) A survey of face recognition techniques. Information Processing Systems5(2):41–68.

[3]. Zou J, Ji Q, Nagy G (2007) A comparative study of local matching approach for face recognition. IEEE Transactions on Image Processing 16(10):2617–2628. [PubMed]

[4]. Subban R, Mankame DP (2014) Human face recognition biometric techniques: analysis and review. Recent Advances in Intelligent Informatics: 455–463.

[5]. 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.

[6]. 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.

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

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

[9]. 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.

[10]. 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.

[11]. E. M. Newton, L. Sweeney, and B. Malin, "Preserving privacy by de-identifying face images," IEEE Trans. Knowl. Data Eng., vol. 17, no. 2, pp. 232–243, Feb. 2005.

[12]. R. Gross, L. Sweeney, F. De la Torre, and S. Baker, "Model-based face de-identification," in IEEE Workshop on Privacy Research in Vision, Los Alamitos, CA, 2006.

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

[14]. B. Moskovich and M. Osadchy, "Illumination invariant representation for privacy preserving face identification," in Proc. IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics, San Francisco, CA, Jun. 2010, pp. 154–161.

[15]. A. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Advances Signal Process., pp. 1–17, 2008.

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

[17]. Adhikari Avishek and Bimol Roy (2007). "Applications of Partially Balanced Incomplete Block Designs in Developing (2,n) Visual Cryptographic Schemes". IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences Vol.E90-A No.5 pp.949-951

