Biometric Face Image Privacy Using Visual Cryptography

Ms. Pawar Sarika D[1]., Dr. Kanade S. G[2].

PG Scholar, Assistant Professor, E & TC Engineering Department TSSM'S, BSCOER, Narhe, Pune, India

[1] sarika2242@gmail.com

[2] sanjaykanade@gmail.com

Abstract *— Visual cryptography is cryptographic method allowing data to be stored in encrypted format were any individual can decrypt such data by sight reading of human if accurate key images are used.Biometric deals with automatic identification of any individual based on physical or behavioral characteristics of individual. Preserving privacy in biometric data such as face images which are stored in central database are important. The paper deals with the work based on visual cryptography to provide privacy to biometric data such as iris codes, fingerprint images and face images. Visual cryptography is a method in which a private image is encrypted into the sheets which are incapable of revealing information about original private image, if used independently. Biometric information are stored in the centralized database and are vulnerable to attacks which can modify original content and authorized owner may not be able to access the resource. To tackle this issue visual cryptography schemes can be applied to secure privacy of digital biometric information. In this method the private image or face is dithered in to two different host images i.e., sheets and are stored in separate data servers so as to ensure that the original image can get retrieved only by accessing both sheets together at a time and single sheet will not be able to reveal any information of private image.*

Keywords- *De-identification, biometric privacy,face, fingerprint, Iris Codes, privacy, visual cryptography*

I. INTRODUCTION

BIOMETRICS is the metric related to human characteristics. It is used in digital world as a form of identification and access control. It is a science of establishing the identity of an individual based on physical or behavioral traits such as iris, face, fingerprints etc .Biometric authentication system works by acquiring raw biometric data from an individual , extracting a feature set from the data, and comparing the feature set against the templates stored in a database in order to identify the individual or to verify a claimed identity. During enrolment process biometric data is stored in the database server to provide identification of individual. For providing privacy to biometric data visual cryptography is used. Visual cryptography is a digital technique which encrypts the visual information in such a way that only human vision can decrypt it. It is used to preserve privacy of biometric information.

Visual Cryptography uses two host images. In this one image has random pixels and the other image has the secret data. It is not possible to get the private information from one of the images. Original information can only be retrieved by using both images simultaneously. In this process the biometric image is decomposed and other two noise like images i.e., sheets are created. In case of private face image, it is decomposed into two independent host images In this paper a system is proposed to biometric information by applying visual

cryptography technique. It has been applied on to the private face image information to secure it from attacks and provides extra authentication.

II.RELATED WORK

Naor and Shamir's [2] proposed basic visual cryptographic scheme. It is the best technique to secure information. In this scheme the visual cryptographic scheme (VCS) is developed. Its performance depends on contrast and pixel expansion. There are many papers which proposes the VCS having pixel expansion value 1[3-4].

S. Prabhakar, S. Pankanti, A. K. Jain [5] proposed a biometric system used to recognize an individual by feature vector which are being derived from some specific behavioral or physiological character possessed by that individual. The characters provides convenience, reliability, universality, etc. As biometric data is non-replaceable and not secret, the biometric systems do not provide security of individual's information.

Ateniese *et al.* [6] introduced such a framework called the extended VCS. Nakajima and Yamaguchi [7] proposed an extended Visual cryptography on gray scale images. The paper provides with a framework which encodes natural images which is known as the gray-level extended visual cryptography scheme (GEVCS).This extended VCS secure face image for grayscale images. It also enhance targeted image contrast.

III.PROPOSED SYSTEM

Securing individual information is most important in biometric systems, hence GEVCS is used to decompose private image in two host images in visual cryptography for authenticating secure biometric information. It works by changing the range of original and host image, by transferring the image in to half toned image and after that we have apply Boolean operation on half toned pixels of original image and host image. The proposed system consist of following modules as shown in the fig.1

A. Enrolment Module

B. Authentication Module

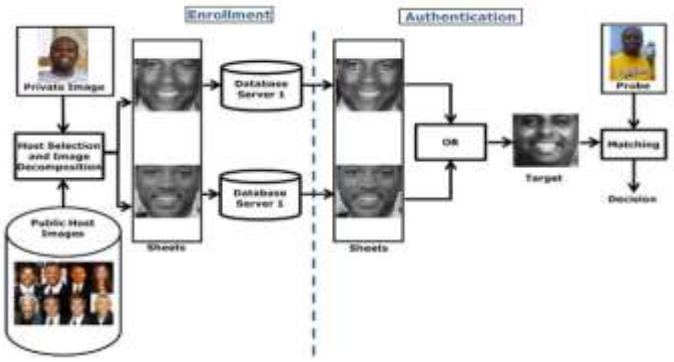

Fig. 1 System Architecture for de-identifying and storing a face image

A. Enrolment Module

In the enrolment process, the private image is scrambled and sent to a trusted third-party. As the trusted party receives information, the original scrambled image is decomposed in two parts called sheets which consists of specific number of pixels and original image is discarded. These sheets are stored in separate database servers so as to ensure that their identities do not get revealed to either server. To make the private image secure, it is divided into two images and stored in two separate data servers.

B. Authentication Module

In the authentication process, the trusted party sends a request to each of the two server and the respective sheets are transmitted to it. Sheets are superimposed (i.e., overlaid) in order to reconstruct and retrieve the scrambled image. This can be done only if both the sheets are retrieved simultaneously. Here private image i.e gray level image converted into binary image is called as halftoned image. If the two sheets are matched then only the original gets

retrieved and the individual is able to access the resource. The XOR operator is used to superimpose the two noisy images and fully recover the original data.

IV. EXPERIMENTS AND RESULTS

VCS allows us to encode a secret image into two sheet images. These sheets appear as a random set of pixels. The sheets could be reformulated as natural images known as host images.

1) Secret image - The original image that has to be hidden. In our application, this is the private biometric image.

2) Share - Each pixel is encrypted by collections of black-and-white subpixels. These collections of subpixels are known as shares.

Images have been taken from different sources of database by online. Here software MATLAB 13version is used. Some sample face image of a person are taken and croped. Shares are generated by using gray level exteneded visual cryptography scheme to hide the image.

Images for encoding

Images for decoding

Results of Decryption

In this way the host images are decoded to get the two host shear images i.e., shear1 (image0) and shear2 (image1).When these two images are overlaid on each other then the orignal private image (image 2) is retrived as shown above.

V.DISCUSSIONS

The experimental results demonstrate the difficulty of exposing the identity of the secret image by using only one of the sheets; further individual sheets cannot be used to perform cross-matching between different applications. Method to protect privacy of face images by decomposing it into two independent host (public) face images. Original face image can be reconstructed only when both host images are available. Either host image does not expose the identity of the original face image.

VI.CONCLUSION

The paper explores the possibilities of using visual cryptography for preserving the privacy to biometric information's (face database). VCS is used to encrypt the private image in the selected host images. It is observed that the reconstructed images are similar to the original private image. The privacy of digital biometric data stored in database like fingerprint, face image, iris code can be achieved. In future same kind of scenario can be applied for the video based biometrics and to verify the authentication for both video based biometrics and still image.

ACKNOWLEDGEMENT

I would like to thank all people who help me in different way. Especially, I am thankful to my guide Dr. Kanade S. G. and P.G. Co-ordinator Prof. Pansambal B. H. for their continuous support and guidance in my work. Also, I would like to thank H.O.D. of E & TC(Signal Processing)Engg. Department,Prof. Pawar D. B. for motivating me.

REFERENCES

[1]. Arun Ross and Asem Othman," Visual Cryptography for Biometric Privacy",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1, MARCH 2013

[2]. Moni Naor and Adi Shamir, "Visual cryptography" .In Proceedings of the advances in cryptology– Eurocrypt, 1-12,1995.

[3]. H.-C. Hsu, T.-S. Chen, Y.-H. Lin,"The ring shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing". In Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taipei, Taiwan, pp. 996–1001, March 2004.

[4]. F. Liu1, C.K. Wu X.J. Lin , "Colour visual cryptography schemes". IET Information Security, 2(4), 151-165, 2008.

[5]. S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric recognition: security and privacy concerns". In Proceedings of the IEEE Security & Privacy, 33-42, March/April 2003.

[6]. 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.

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