Securing the Images Using Biometric Cryptography Technique

K.Nandakumar[#1] D.Prabakar[#2] Dr.S.Karthik[#3]

[1#] *Pg Scholar, Dept of CSE, SNS College of Technology- India*
[2#] *Assistant Professor, Dept of CSE, SNS College of Technology- India*
[3#] *Professor & Dean, Dept of CSE, SNS College of Technology-India.*

***ABSTRACT* - A biometric authentication system operates by acquiring raw biometric data from a subject, extracting a feature set from the data and comparing the feature set against the templates stored in a database in order to identify a person or to verify a claimed identity. The template data in the database is generated during enrolment and is often stored along with the original raw data. This work explores the possibility of using visual cryptography without pixel expansion for imparting privacy to biometric data such as fingerprint images, iris codes, and face images. In the case of faces, a private face image is dithered into two host face images that are stored in two separate database servers 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. Two schemes such as Multiple Secrets without pixel expansion and Multiple-level visual secret-sharing scheme without image size expansion. The First approach has the three phases for encryption scheme such as dividing and separating process, sticking process and camouflaging with maximum block density process. The Second approach uses histogram width-equalization and histogram depth-equalization. Histogram depth equalization is used to obtain better reconstructed secret image.**

Key Words – Multiple Secrets, Depth-equalization, Pixel Expansion.

I. INTRODUCTION

Biometrics is defined as the science of establishing the identity of an individual based on physical or behavioral traits, since each person is believed to have a unique biometric, if this biometric data is compromised, it is not possible to replace it. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense [1][9]. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread. One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or cryptosystem. Cryptosystems (e.g. El-Gamal encryption) are designed to provide particular functionality (e.g. public key encryption) while guaranteeing certain security properties (e.g. chosen-plaintext attack (CPA) security in the random oracle model). Cryptosystems use the properties of the underlying cryptographic primitives to support the system's security properties. Of course, as the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem can be derived from a combination of several more primitive cryptosystems. In many cases, the cryptosystem's structure involves back and forth communication among two or more parties in space (e.g., between the sender of a secure message and its receiver) or across time (e.g., cryptographically protected backup data). Such cryptosystems are sometimes called cryptographic protocols [10][15].

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear [5].

II. PREVIOUS WORK

The existing system uses the predefined visual cryptography with pixel expansion so that the reconstructed image will be twice of its original width, the pixel expansion can affect the performance of the system due to loss in image clarity.

The existing system uses single private image during encryption process [7]. Davida and Ratha proposed storing a transformed biometric template instead of the original biometric template in the database. This was referred to as a private template or a cancelable biometric Feng proposed a three-step hybrid approach that combined the advantages of cryptosystems and cancelable biometrics. Newton and Gross introduced 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.

Bitouk 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[6][4]. However, in the case of face swapping and aggressive de-identification, the original face image can be lost. Moskovich and Osadchy proposed a method to perform secure face identification by representing a private face image with indexed facial components extracted from a public face database Arun Ross, Asem Othman proposed the use of visual cryptography is explored to preserve the privacy of biometric data (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 the following drawbacks are made Pixel Expansion exists and Private face image can be obtained using aggressive de-identification method.

III.PROPOSED WORK

Two schemes such as Multiple Secrets without pixel expansion and Multiple-level visual secret-sharing scheme without image size expansion. Multiple secrets without pixel expansion approach has three phases 1.dividing and separating process, 2.sticking process,3 camouflaging with maximum block density process for encryption. In decryption process, first stacking with two share images and then stacking first share image and second share with 180 degree. Histogram width-equalization and histogram depth-equalization are used in the second approach. This method usually increases the global contrast of many images, especially when the usable data of the image is represented by close contrast values. Through this adjustment, the intensities can be better distributed on the histogram. This allows for areas of lower local contrast to gain a higher contrast. Histogram equalization accomplishes this by effectively spreading out the most frequent intensity values. Histogram depth-equalization often has better reconstructed secret image quality. A series of experiments on the XM2VTS and IMM face databases confirm the following: 1) the possibility of hiding a private face image in two host face images, 2) the successful matching of face images reconstructed from the sheets; 3) the inability of sheets to reveal the identity of the private face image; 4) using different pairs of host images to encrypt different samples of the same private face; and 5) the difficulty of cross-database matching for determining identities. A similar process is used to de-identify fingerprint images and iris codes prior to storing them in a central database. To overcome the previous works and having the advantages of Multiple secrets are secured and High quality reconstructed image is obtained.

IV SCOPE OF THE WORK

Biometrics is defined as the science of establishing the identity of an individual based on physical or behavioural traits, since each person is believed to have a unique biometric, if this biometric data is compromised, it is not possible to replace it. In order to overcome the security and privacy problems Visual cryptography scheme can be used for biometric data such as fingerprint images, iris codes, and face images[12][18]. In the case of faces, a private face image is dithered into two host face images (known as sheets) that are stored in two separate database servers 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.

A. Gray-Level Extended Visual Cryptography Scheme (GEVCS)

VCS allows one to encode a secret image into sheet images, each revealing no information about the original. Since these sheets appear as a random set of pixels, they may pique the curiosity of an interceptor by suggesting the existence of a secret image. To mitigate this concern, the sheets could be reformulated as natural images and such a framework is known as Extended VCS. Extended visual cryptography on gray scale images (GEVCS) is used to enhance the contrast of the target images [14]. Digital halftoning is a technique for transforming a digital gray-scale image to an array of binary values represented as dots in the printing process. Error diffusion is a type of halftoning technique in which the quantization error of a pixel is distributed to neighbouring pixels which have not yet been processed.

B.Securing Iris and Fingerprint Templates

The use of basic visual cryptography for securing fingerprint and iris templates is suggested. Moreover, basic VCS leads to the degradation in the quality of the decoded images, which makes it unsuitable for matching process. The overlaying or superimposing operation in visual cryptography is computationally modelled as the binary OR operation which causes the contrast level of the target image to be lowered. Loss in contrast in target images could be addressed by simply substituting the OR operator with the XOR operator .Furthermore, the target image can be down-sampled by reconstructing just one pixel from every 2x2 block [3].

C. Securing Private Face Images

The proposed approach essentially selects host images that are most likely to be compatible with the private image based on geometry and appearance. Therefore, an Active Appearance Model (AAM) that characterizes the shape and texture of the face is utilized to determine the similarity between the private face image and candidate host images. The steps for building the AAM and using it for locating predefined landmarks on face features. The steps that are involved in building up of AAM are Annotate the Training Set, Building the Shape Model, Building the Texture Model and Building the Combined AAM[16].

D. Visual Secret Sharing Scheme for Multiple Secrets

The main concept of the original Visual Secret Sharing (VSS) scheme is to encrypt a secret image into ‘n’ meaningless share images. It cannot leak any information of the shared secret by any combination of the n share images except for all of images. The Visual Secrets Sharing Scheme for Multiple Secrets (called VSSM scheme) is intended to encrypt more than one secret image into the same quantity of share images to increase the encryption capacity compared with the original VSS scheme. However, all presented VSSM schemes utilize a pre-defined pattern book with pixel expansion to encrypt secret images into share images. In general, it leads to at least 2x time’s pixel expansion on the share images by any one of the VSSM schemes. Thus, the pixel expansion problem becomes more serious for sharing multiple secrets. A novel VSSM scheme that can share two binary secret images on two rectangular share images with no pixel expansion has been proposed illustrated in figure 1. The proposed scheme adopted two rectangular share images to share two rectangular secret images [17].

The rotation degree was 180 degree for revealing the second secret image. As with the previous schemes, encrypting and decrypting processes were needed. In the proposed scheme, encryption included 3 processes, they are Dividing and Separating Process (DSP), Sticking Process (SP), Camouflaging with maximum block density process (CMP).

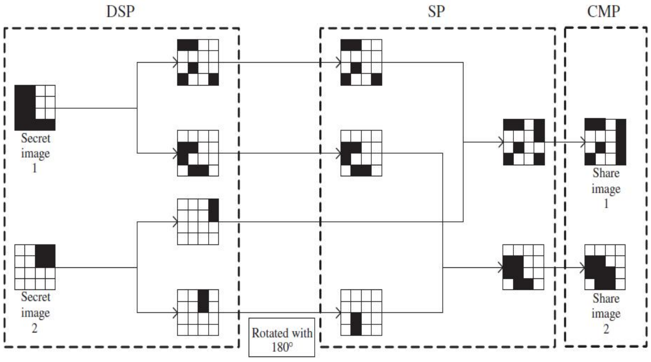

Fig. 1 the Encryption Process Chart of Proposed Scheme

E. Dividing and Separating Process (DSP)

In DSP, the first function is to divide each secret image into blocks with n x n size, and the second function was to separate each block of the secret image into two subsets without intersection according to the black pixel on one n x n block. At the beginning, two empty share images (i.e., the pixel color is white) with a size equal to that of the secret image must be generated. Then, each secret image must be divided into K blocks with n x n size that is K = (h/n) x (w/n). According to the position of each black pixel and the sum of black pixels on the block, one block can be randomly separated to two subsets without any one black pixel being overlapped, and the difference in the number of black pixels between the two subsets must be equal to or less than one. For one block, the two subsets are noted as C^{q} and C^{q+1} then,

$$|H(C^{q}) - H(C^{q+1})| <= 1. \qquad (Eqn.\ 1)$$

F. Sticking Process

In SP, the function was to stick the subsets obtained by DSP to generate the share images, and two subsets of secret image SE1 were stuck to share images S1 and S2, respectively. The first subset of SE2 was directly stuck on the corresponding position of S1 while, the second subset of SE2 was rotated with 180 degree and stuck to the corresponding position of S2.

The sticking operation executes logic ‘‘OR” operation between the separated subset and the share images during the sticking process depicted in figure 2. The goal is to build the patterns of two blocks for share images S1 and S2 [2]. The sticking results are generated according to the decrypting function. By the defined decrypting process in our proposed scheme, secret image SE1 is revealed by directly stacking share images S1 and S2. But, it needs to rotate the share image S2 with 180_ angle and stack with S1.

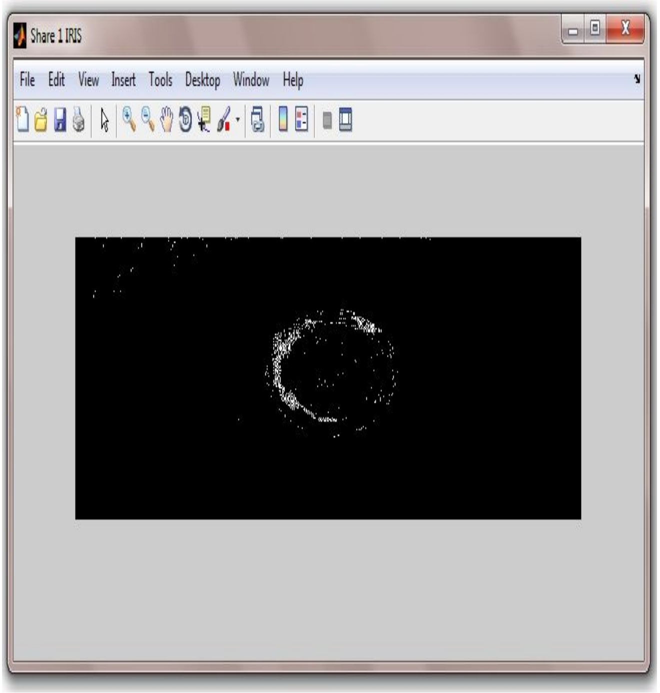

Fig. 2 Share images during the sticking process

According to the rule of the decrypting process, the two subsets, C1 and C3, separated from DSP for secret images SE1 and SE2, respectively, can be stuck together to build one corresponding block for share image S1. In order to build the corresponding block of share image S2, the whole matrix, with C4 separated from share image S2 by DSP, must be rotated 180 degree and stuck with the corresponding block of C2, which is another separated subset of S1, to generate share image S2. It was obvious that every pixel was moved from one position to another related position by the 180 degree rotation angle. For example, the pixel on the right-bottom position was moved to the left-top position, and vice versa.

G .Camouflaging with Maximum block density process

The function of the last process, CMP, was to camouflage two share images to make the density of the black pixel on each block of one share image to be equal by referencing the maximum block density of all blocks. In order to make the share image meaningless to anyone but an unauthorized user, two camouflaging processes must be executed for every block of two share images obtained from the sticking process [8]. Based on the maximum of block density, the camouflaging process makes the black pixel density of every block equal, so that every block appears to have the same pattern and the whole image will be a meaningless image. In the decrypting process, the first secret image was revealed by directly stacking share image S1 and share image S2. To reveal the second secret image, share image S1 was stacked and share image S2 with a rotated 180 degree.

VI. CONCLUSION

This Project explored the possibility of using visual cryptography for imparting privacy to biometric templates. Thus the Multiple Secrets without pixel expansion and Multi level visual secret sharing scheme without image size expansion is used to obtain high quality target image and hence the problem of pixel expansion is reduced. The system’s security is also improved by hiding multiple secrets in same number of share images. The future works covering of using Multi level visual secret sharing technique the pixel expansion rate is reduced and high quality target image is obtained which indeed increases the storage requirements for sheets and the target image. No other techniques are currently available to overcome this difficulty. In future it can be achieved by using techniques that reduces the size of sheets and share images.

ACKNOWLEDGMENT

Our Sincere thanks to the Professor & Dean Dr.S.Karthik, his valuable suggestion and thoughts is to motivated publish this paper and our beloved Professor & HOD Dr.T.Kalaikumaran, of department of computer science and engineering, his excellence and suggestion is very useful towards this paper to carry out.

REFERENCES

[1] Agrawal. N and Savvides. M, (2009), “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, vol. 0, pp. 85–92.

[2] Anil K. Jain and Umut Uludag, (2008), “Hiding Biometric Data”, IEEE Trans. Pattern Analysis And Machine Intelligence, Vol. 25, No. 11.

[3] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, (2008), “Biometric Template Security”, EURASIP Journal on Advances in Signal Processing.

[4] Arun Ross and Asem Othman, (2011), “Visual Cryptography for Biometric Privacy,” IEEE trans. Information forensics and security, vol. 6, no. 1.

[5] Ateniese.G, Blundo.C, Santis.A, and Stinson.D, (2010), “Extended capabilities for visual cryptography,” Theor. Comput. Sci., vol. 250, no. 1–2, pp. 143–161.

[6] Bitouk.D, Kumar.N, Dhillon.S, Belhumeur.P and Nayar.S.K, (2008), “Face swapping: Automatically replacing faces in photographs,” ACMTrans., vol. 27, no. 3, pp. 1–8.

[7] Dong.J and Tan.T, (2008), “Effects of watermarking on iris recognition performance,” in Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, pp. 1156–1161.

[8] Gross.R, Sweeney.L, De la Torre.F, and Baker.S, (2007), “Model-based face de-identification,” in IEEE Workshop on Privacy Research in Vision, Los Alamitos, CA.

[9] Jain.A, Nandakumar.K and Nagar.A, (2008), “Biometric template security,” EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics.

[10] Maltoni.D, Maio.D, Jain.A, and Prabhakar.S, (2008), “Handbook of Fingerprint Recognition”. Secaucus, NJ: Springer-Verlag New York, Inc.

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

[12] Nakajima.M and Yamaguchi.Y, (2012), “Extended visual cryptography for natural images,” J. WSCG, vol. 10, no. 2, pp. 303–310.

[13] Naor.M and Shamir.A, (2010), “Visual cryptography,” in EUROCRYPT, pp. 1–12.

[14] Newton.E.M, Sweeney.L and Malin.B, (2007), “Preserving privacy by de-identifying face images,” IEEE Trans. Knowl. Data Eng., vol. 17, no. 2, pp. 232–243.

[15] Prabhakar.S, Pankanti.S, and Jain.A, (2011), “Biometric recognition: Security and privacy concerns,” IEEE Security Privacy, vol. 1, no. 2, pp. 33–42.

[16] Ratha N.K, Connell J.H, Bolle.R.M, (2011), “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, Vol 40, No 3.

[17] Soutar.C, Roberge.D, Stoianov.A, Gilroy.R, and Kumar.B, (2009), “Biometric encryption,” in ICSA Guide to Cryptography. New York: Mc Graw-Hill.

[18] Thuraisingham.B and Ford.W, 2007), “Security constraint processing in a multilevel secure distributed database management system,” IEEE Trans. Knowl. Data Eng., vol. 7, no. 2, pp. 274–293.