Technique for Halftone Images without Pixel Expansion Using an Extended Visual Cryptography Scheme

[1]Vidya Mahadik, [2]Rani Sangale, [3]Pooja Murame, [4]Prof. Deepali Ahir

[1,2,3,4] B.E Computer, Modern Education Society's college of Engineering Pune, India

Abstract: **Visual cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. In extended visual cryptography, the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual cryptography and biometric security techniques. In this paper, we propose a method for processing halftone images that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image is the same as for the original halftone secret image. The resulting scheme maintains the perfect security of the original extended visual cryptography approach. It is another form of cryptography in which secret communication is done in the form of images. This can be used to protect the biometric templates in which the decryption doesn't require any complex computations; it is done by human visual system. Using this visual cryptography the biometric data capture from the authorized user. This original image is divided into two shares .Each share stored in two different databases. When both images are simultaneously available then only we can get the original image. The individual share do not reveal any information about the original image**

Keywords: **cryptography, image processing, visual cryptography, secret sharing.**

I. INTRODUCTION

Biometric is one of the authentication system it comes from the Greek words 'bios and metricos' which means 'life measure'. It is more reliable, consistent and also user friendly. So it is used for many application such as computer login control, passport control, border crossing, secure e-banking, ATM, credit cards, airport, etc.

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioural traits such as face, fingerprints, iris, etc. The working of biometric authentication system acquires 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 the subject or to verify a claimed identity.At the same time there is a possible to intruder can access the database which stored the biometric data. So the security and privacy of biometric system is a major concern due to their issues like fake biometric, override matcher and etc. The biometric data classified as physiological or behavioural. Physiological biometrics based on the physical part of the body such as fingerprint, iris, eye retina, face, palm, hand. Behavioural type is based the behaviour of human such as voice, signature and keystroke.

Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message.

Visual cryptography is introduced by Noar and Shamir. It is another form of cryptography in which secret communication is done in the form of images. This can be used to protect the biometric templates in which the decryption doesn't require any complex computations; it is done by human visual system. Using this visual cryptography the biometric data capture from the authorized user. This original image is divided into two shares .Each share stored in two different databases. When both images are simultaneously available then only we can get the original image. The individual shares do not reveal any information about the original image.

1.1 Problem Statement

Explore the visual cryptography to preserve the privacy of Biometric data by decomposing original image into two images in such a way that the original image can be revealed only when both images are simultaneously available.

There are various types of attacks on Biometric Systems as follows:

1. Fake Biometric

Attack on the sensor. Sensor can be overridden by presenting fake . Like a fake finger, face mask or a copy of signature.

2. Replay Old Data

The Attack on the channel between the sensor and the feature extractor. Biometrics which was submitted can be resubmitted or replayed by bypassing the sensor. Like an old copy of fingerprint or face image.

3. Override Feature Extractor

Feature extractor can be override by attacking it and forcing it to produce feature values selected by the hacker.

4. Override Matcher

Attack on the matcher. Matcher can be overridden by attacking it and forcing it to produce high or low matching score irrespective of the input.

1.2 Solution

Following approach can be used to obtain a solution for the above mentioned problem.

Steganography Techniques for Biometric Template Security

Watermarking Techniques for Biometric Template Security

Visual Cryptography Technique for Biometric Template Security

II. SYSTEM MODEL

2.1 Architecture for Visual Cryptography Scheme

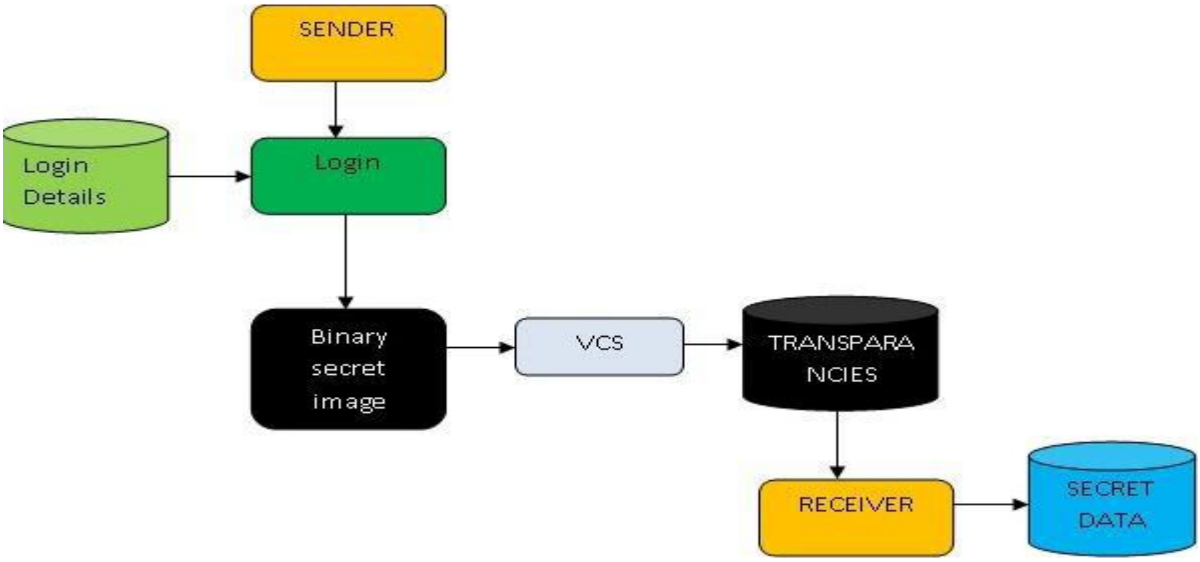

Fig 2.1 System Model

Visual cryptography (VC) scheme is a type of secret sharing scheme of cryptography that can split secret information or image into *n* shares and recover them by superimposing the shares. The shares of the image can be easily decrypted by human visual system without any special computation because it doesn't rely on any specialized hardware or software, can be decrypted with human eye. In our work space in case of information or images, sometimes illegal duplication, unauthorized manipulation etc. has been happening which causes threats for confidential ones. To protect important information or images against these types of abuses, VC provides a reliable solution.

III. EXTENSIVE TECHNICAL RESEARCHES

3.1 Visual Cryptography Scheme

One of the best known techniques to protect data such as biometric Templates is cryptography. It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system.

Using this visual cryptography the biometric data capture from the authorized user. These original images are divided into two shares .Each share stored in two different or same databases. When both images are simultaneously available then only we can get the original image. The individual shares do not reveal any information about the original image. This technique is also used for iris codes. So the visual cryptography scheme is more secure for biometric template security.

But it requires more space for storing sheets due because of pixel expansion.

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 Ateniese introduced new framework known as the extended VCS.

3.2 GEVCS

Nakajima and Yamaguchi proposed a theoretical framework to apply extended visual cryptography on gray scale images (GEVCS). The preparation of a gray scale image for use in visual cryptography involves 3 steps.

The first step is the transformation of a gray scale image into a halftone image and partitioning the halftone image into non-overlapping blocks of 2 × 2 pixels.

Then, the halftone image is divided into a number of overlapping squares of four 2 × 2 blocks. Each grouping of 4 blocks is referred to as a cluster.

In the second step, the number of black pixels in each cluster from the halftone image are counted and saved in a template. This number is the threshold value for that cluster. The step then classifies all the secret blocks containing 1 black (resp. white) pixel. If the secret block contains 1 black (resp. white) pixel, it is converted to a white (resp. black) block. The image obtained from this step is referred to as the initial processed image.

The third step starts from the first block in the top left of the first cluster of the initial processed image. The processing of the blocks in each cluster starts from the top left block, then moves from left to right and top to bottom in raster format.

When the first candidate block in a cluster is identified, the numbers of black pixels in the cluster are counted. The idea is to keep the number of black and white pixels in each cluster of the initial processed image as close as possible to the corresponding threshold value from the cluster of the original halftone image. Therefore the number of black pixels in the case of changing the candidate block to a black or white block is computed and is compared to the threshold value that was derived for the same cluster in the original halftone image. If the corresponding candidate block converts to a black block, 2 pixels will be added to the number of black pixels in a cluster and if the candidate block turns to white block, 2 black pixels will be deducted from a cluster. The conversion is based on the smallest to black or white produces the same difference, the block randomly converts to either a black or white block. Difference between the threshold and the number of black pixels in the image being processed. If changing the candidate block to black makes this difference smaller, the candidate block is converted to a black block. Similarly, if turning the candidate block to white makes this difference smaller, the block converts to a white block. In the case that turning the candidate

3.3 Digital Halftoning

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. In this section, we consider the application of visual cryptography to grayscale images by first converting the images to a binary image using a halftoning algorithm. After creating a halftone image, in order to preserve the image size when applying visual cryptography and extended visual cryptography, simple methods can be applied.

Halftoning is a method for creating the illusion of continuous tone output with a binary device. Effective digital halftoning can substantially improve the quality of rendered images at minimal cost. Following are the methods of Digital half toning.

1) Thresholding

2) Constant Threshold

3) The Minimum Squared Error Solution

4) Ordered Dither

3.3.1 Ordered Dither

• This creates the perception of continuous variations of gray.

• An N × N index matrix specifies what order to use.

I(i, j) For a constant gray level patch, turn the pixel “on “in a specified order.

=[0 1 2 3]

• Pixels are turned on in the following order.

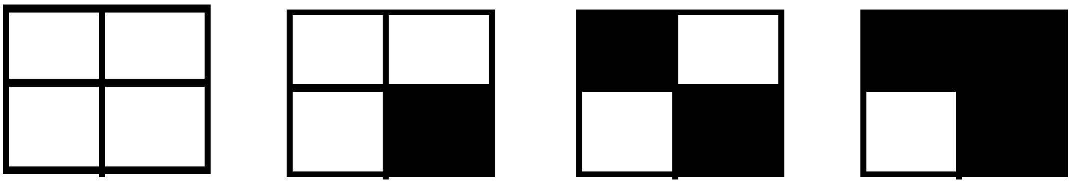

Figure: 3.3.1 2x2 index matrix

Application

This approach is particularly applicable in situations where a moderate degree of security is required when sharing sensitive secret data or file over the Internet. Visual cryptography can be used to protect secrecy or it may be used to ensure that a given subset of compromised principals can neither retrieve the secret, nor can they prevent honest principals from receiving the secret.

Future Enhancements

- It can be used at all security related institutions like military, offices, confidential laboratories.
- The system will be developed with automatic functionality.

IV. CONCLUSION

Thus 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.

REFERENCES

[1] IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1, MARCH 2011, Arun Ross, Senior Member, IEEE, and Asem Othman, Student Member, IEEE.

[2] 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.

[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] 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.

[5] B. Thuraisingham and W. Ford, "Security constraint processing in a multilevel secure distributed database management system," IEEE Trans. Knowl. Data Eng., vol. 7, no. 2, pp. 274–293, Apr. 1995.

[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] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Secaucus, NJ: Springer-Verlag New York, Inc., 2003.

[8] S. Prabhakar, S. Pankanti, and A. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[9] Ross and A. A. Othman, "Visual Cryptography for Biometric Privacy", IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, 2011.

[10] Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing,vol. 15, no. 8, pp. 2441-2451, 2006.