ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (722-726), Month: April - June 2015, Available at: www.researchpublish.com

Extended Visual Cryptography For Halftone Images Without Pixel Expansion

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

[1,2,3,4] Department of Computer Engineering MES College of Engg, 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.**

1. INTRODUCTION

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.

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.

2. RELATED WORK

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.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (722-726), Month: April - June 2015, Available at: www.researchpublish.com

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.

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. METHODOLOGY

Architecture for Visual Cryptography Scheme

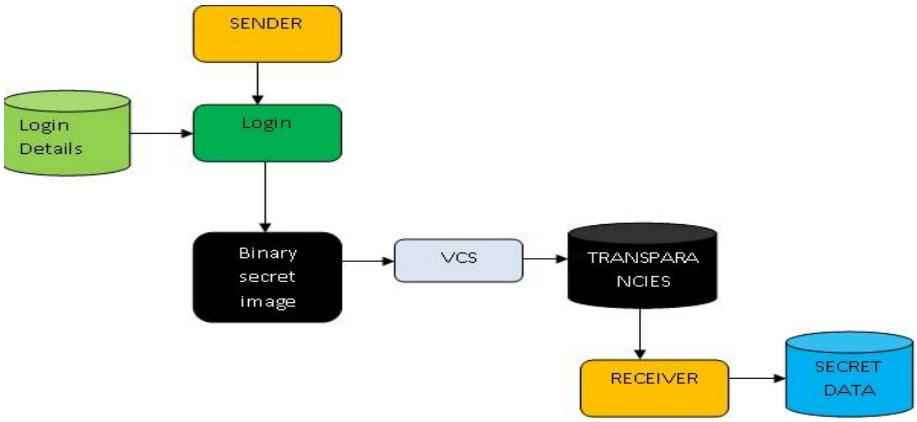

Figure.1 System Architecture

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

Modules:

- Module 1:Extraction of face image from database
- Module 2:Division of face image in two different data sheets
- Module 3:Storage of sheets at two different database servers
- Module 4:Extraction of sheets saved at two different database servers
- Module 5:Oring of two sheets
- Module 6:Matching with two original image

Algorithms:

The steps in which algorithms are executed.

For Encryption:

a) Rescaling:

1) Read the original Image.

2) Define the new height and width of rescaled image.

3) Create Graphics2D object and give the rescaled image.

4) Draw the original image on the rescaled image.

5) return the rescaled image.

b) Gray Scale Conversion:

1) Read the original image.

2) Define a new blank image of same height and width of original image. This blank image will be our grey image.

3) for i=0 and i < original image , repeat step 5,6,7

4) for j=0 and j < original image height , repeat step 5,6,7

5) read the Red,Green and Blue component individually for pixel at position(i,j).

6) grey = 0.21*Red+0.71*Green+0.07*Blue

7) set grey at position(i,j) in grey image

8) return grey image.

c) Halftoning by Floyd Steningberg

Pseudo Code

1) Read the original image.

for each y from top to bottom

for each x from left to right

oldpixel := pixel[x][y]

newpixel := find_closest_palette_color(oldpixel)

pixel[x][y] := newpixel

quant_error := oldpixel - newpixel

pixel[x+1][y] := pixel[x+1][y] + quant_error * 7/16

pixel[x-1][y+1] := pixel[x-1][y+1] + quant_error * 3/16

pixel[x][y+1] := pixel[x][y+1] + quant_error * 5/16

pixel[x+1][y+1] := pixel[x+1][y+1] + quant_error * 1/16

d) Encryption for EVCS:

I have highlighted the alog on page 11 and 12 in attached pdf

e) Decryption for EVCS:

1) Read the two share images.

2) Define a new blank image of same height and width of original image. This blank image will be our recovered Secret image.

3) for i=0 and i < original image , repeat step 5,6,7,8

4) for j=0 and j < original image height , repeat step 5,6,7,8

5) pixel1 = pixel value at position(i,j) at shareImage One

6) pixel2 = pixel value at position(i,j) at shareImage Two

7) secretPixel = minimum(pixel1,pixel2)

8) set secretPixel at position(i,j) in Secret image

9) return secret image.

f) Pattern Matching:

1) Read the secretImage

2) Read the uploadedImage

3) Set totalCount=0 and match=0;

4) for i=0 and i < original image , repeat step 6,7,8,9

5) for j=0 and j < original image height , repeat step 6,7,8,9

6) pixel1 = pixel value at position(i,j) at secretImage

7) pixel2 = pixel value at position(i,j) at uploadedImage

8) if(pixel2==255) increment totalCount and goto step 8 else repeat

9) if(pixel1==255) increment match

10) matchPercent = (match/totalCount)*100.

11) if matchPercent>24 return user authentication true

12) if matchPercent<=24 return user authentication false

4. EXPEREMENTAL ANALYSIS

We will do this experiment with the images. 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. 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. In our system we use digital halftone algorithm, EVCS techniques, Half toning by Floyd Steningberg algorithm. Our proposed system will check the authenticated user.

5. 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.

6. MOTIVATION

Author would like to take this opportunity to express our profound gratitude and deep regard to our guide prof. Deepali Ahir for her exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. Her valuable suggestions were of immense help throughout our project work. Her perceptive criticism kept us working to make this project in a much better way. Working under her was an extremely knowledgeable experience for me.

REFERENCES

[1] Prof.Deepali Ahir,Vidya Mahadik, Rani Sangale, Pooja Murame" Technique For Halftone Images Without Pixel Expansion Using An Extended Visual Cryptography Scheme" International Journal Of Engineering Research And Reviews ISSN 2348-697X (Online) Vol. 2, Issue 4, Pp: (56-60), Month: October - December 2014

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.