A Secure and Verifiable Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares

Shubhangi Khairnar
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune-44

Reena Kharat
Department of computer Engineering,
Pimpri Chinchwad Collage of Engineering
Pune-44

ABSTRACT

Data, information and image security is very important in now days. Data and image encryption is a method for preventing misuse of attackers. Because encryption and decryption is important to securely protect data. Visual cryptography is a technique which is beneficial for defense and security. In the old technique; two secret images convert into halftone image and transmit these images using two shares and stacking these two shares revel the secret images. One drawback of this scheme is can't verify the shares are original or fake. In this paper use the verifiable secret sharing using steganography technique to verify the shares. Proposed scheme can verify the share using steganography and then use XOR visual cryptography for share generation, by using this scheme preventing the misuse of adversaries.

Keywords

Visual Cryptography, Halftone Technology, Multi Secret Sharing, steganography.

1. INTRODUCTION

Now a day's in global data communications, inexpensive Internet connections, and communication technology security is becoming more important issue. Security is basic requirement because global computing is insecure in now a day's. However, secret data can be easily interfered, forged, or attacked by intruders. For the reason of security, secret data is encrypted before transmission.

Blakley and Shamir [1] introduced Secret Sharing Scheme (SSS) to solve the master key problem. To providing the better security of data, Noar [2] proposed a new scheme called Visual Cryptography (VC). The visual cryptography scheme is to divide a secret image into random shares, which reveal no information about

The Visual Cryptography scheme is same like a secret sharing scheme to divide a secret image into random shares, which reveal no information about the secret image. In Visual cryptography image is divided into n number of shares and that are distributed into n number of participants. The important property of visual cryptography is the decryption of the secret images not requires any knowledge of cryptography or complex computation. The decoder can fast recover the secret by using human eyes without the help of computing devices. In this paper, the proposed scheme can use XOR based visual cryptography scheme to encode two secret images into two shares.

Steganography is method for securing the data. Steganography is used to hide the text or image into other image or massage. Using various technique gain steganography like Least Significant Bit Insertion, Masking & Filtering and Algorithms Transformations[4]. In this paper, the proposed scheme can use Least Significant Bit Insertion algorithm for steganography this is simple approach to embedding information in a cover image. This method is use to verify the shares.

2. LITERATURE SURVEY

Noar and Shamir [2] was introduced (2,2) threshold VSS. VC scheme the set of n participants, a secret image S is encoded into n shadow images called shares and each participant gets one share, k out of n participants are needed to combine shares and see secret image. The basic idea of (2,2) Visual Cryptography is, Converted every secret pixel of the original binary image into four sub pixel of two share images and recovered by simple stacking process. This is equivalent to using the logical OR operation between the shares.

Chen and Wu [5] proposed a (2,2)-threshold visual secret sharing scheme for two secret images. Stacking two share images the first secret image is decrypted. Also stacking two share images the second secret image is decrypted and one share image rotated.

Hsu et al [6] proposed another scheme for two secret images are hiding into two share images with arbitrary rotating angles. Easy to rotate share images to get any preferred angle so that round up the share images to become rings.

Duanhao Ou,Wei Sun,Xiaotian Wu[7] proposed a (n,n) XOR-based VC with meaningful shares is carry out systematically by implementing the basic algorithm, where the valid share can be directly generated without additional process. This scheme solves the problems of poor visual quality and pixel alignment in OR based VC scheme. That was easy to implement due to the simple matrix, and there is no pixel expansion and the perfect reconstruction of black pixels.

Rezvan Dastanian and Hadi Shahriar Shahhoseini [8] proposed a new visual cryptography scheme that can transmit the two secret images with the use of two shares. Secret image I appear by stacking two shares and with stacking one of the shares and rotating clockwise with 90 degrees other share appears the secret image II. The size of image is smaller than secret image.

But here by using steganography verify the shares are fake or original. Using proposed scheme preventing the misuse of adversaries.

3. VISUAL CRYPTOGRAPHY

(2, 2) VC Scheme [2] use to encrypt the secret, the original image is split into two Shares such that, original image pixels is replaced with non-overlapping block of two sub-pixels. A white pixel is shared into two equal blocks of sub-pixels. A black pixel shared into two corresponding blocks of sub-pixels. To decrypt the image, stacking both the shares will permit the visual retrieval of the secret. While creating the shares, if the pixel pin the original image is white, then the encoder randomly chooses the first two columns of fig 1.

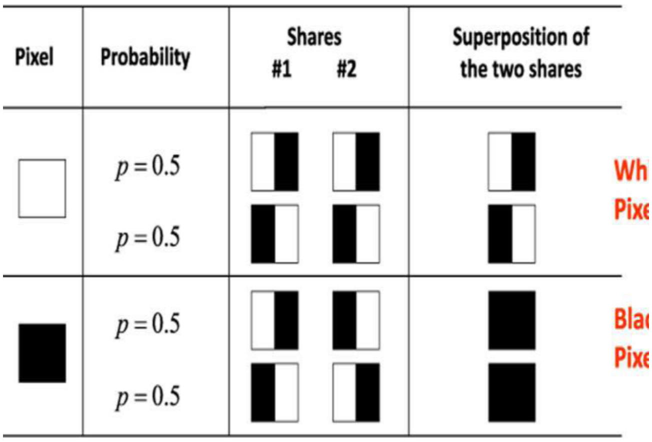

Fig. 1 show 2-out-of-2 VCS scheme with 2 subpixel construction.

In (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig.1 represents the shares of a black and a white pixel. The choice of shares for a white and black pixel is randomly determined. Neither share provides any indication about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When stack the two shares, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if P is a white pixel, we get one black sub pixel and one white sub- pixel.

In this paper, proposed system use XOR VC scheme to generate the share. The XOR schemes have the good contrast property. Actually, their operations can be mathematically represented by the XOR operation. A completely different kind of VCS with reversing was proposed allowing participants to perform reversing operation, which can change black pixels to white pixels and vice-versa. This reversing operation (NOT operation) can be recognized by a copy machine. By this reversing-based VCS, one can perfectly reconstruct the secret by more runs. Because XOR operation can be implemented by four NOTs and three ORs XOR operations can be realized by using a copy machine and transparency.

4. PROPOSED IDEA

In some applications like defense, important information needs to be transmitted in the form of images. This image information may be lost during the transmission. To get the security and reliability image secret sharing can be applied in such applications. Sometimes the shares may be lost in transmission or dishonest participants can modify their shares. In such scenarios verifiability is required for the reconstructed secret which will assure the participants about the accuracy of retrieved secret.

In this paper proposed a new scheme, in this scheme Share a secret two-tone image between two participants, our system uses the two-out-of-two XOR visual cryptography technique to build two share, of 2A*2A for sharing e secret two-tone image. At first, a dealer divides secret image 1 to two shares, share x and share y, and secret image 2 is divided into two shares, share x’, share y’, based on the XOR visual cryptography scheme.

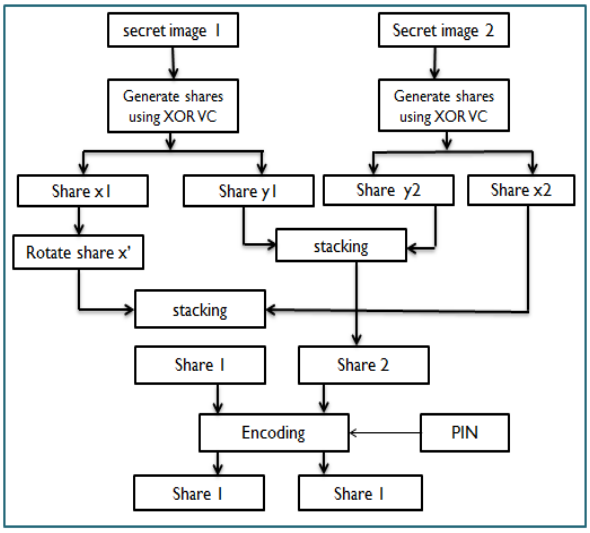

Fig. 2 Flowchart of the proposed scheme for share construction

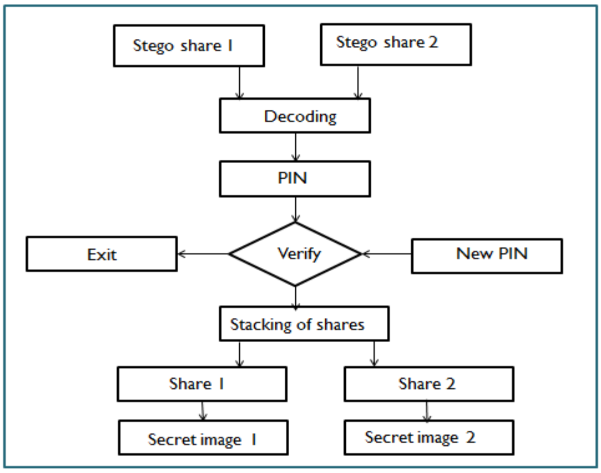

Fig. 3 Flowchart of the proposed scheme for share reconstruction & Verify

As shown in Fig.2 flowchart of the proposed scheme, take two secrete image. Then by using XOR visual cryptography generate the shares of these two images. XOR-based VC with meaningful shares is carrying out systematically by implementing the basic algorithm, where the valid share can be directly generated without additional process. This scheme solves the problems of poor visual quality and pixel alignment in OR based VC scheme. That was easy to implement due to the simple matrix, and there is no pixel expansion and the perfect reconstruction of black pixels.

To make share 1, dealer stacks share x’ with 90 degrees rotation in counterclockwise on share x and for share 1, share y stacking on share y’. Dealer distributes share 1 and 2 between two participants. After generating share 1 and share 2 add one PIN number into those shares. This encoding process is done by using steganography and generates two stego shares1 & 2. At the time of decoding extract the PIN number if PIN number is correct then share is valid if not then exit the process. After share verification for decryption with present two participants, by stacking share 1 and 2, secret image 1 appears and stacking share 1 on share 2 with 90 degrees rotation in clockwise help appear secret image 2.

5. RESULTS

This section shows the implementation results of the proposed scheme for share verification using steganography and XOR visual cryptography. Select two binary secret images shown in Fig. 4

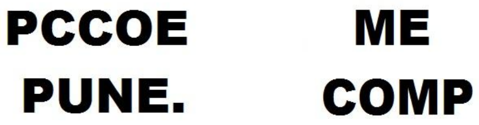

Fig. 4 (1) secret image 1, (2) secret image 2

Select two binary secret image then by using XOR visual cryptography generate two shares, share x and y and binary secret image 2 into share x', y' with XOR VC. Then with stacking share x, share y' with 90 degrees rotation in counterclockwise make share 1, and Stacking share y and y' makes share 2.

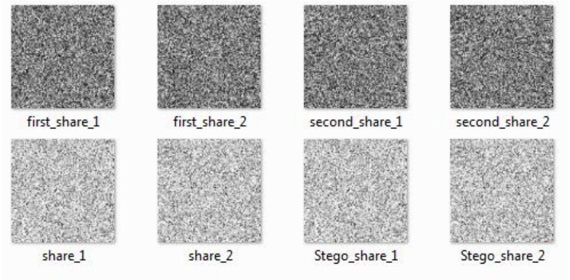

Fig.5 Generated share

After generating share 1 and share 2 add one PIN number into those shares. This encoding process is done by using steganography and generates two stego shares1 & 2. At the time of decoding extract the PIN number if PIN number is correct then share is valid if not then exit the process

For decryption it is sufficient to stack share 1 on share 2 that makes secret image 1 and for decryption of secret image 1 share 1 with 90 degrees rotation in clockwise stack on share 2.

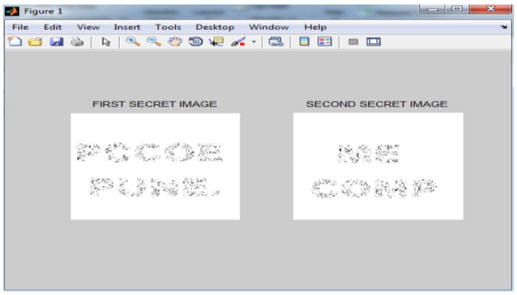

Fig. 7 Extract original images

At the time of decoding extract the PIN number if PIN number is correct then share is valid if not then exit the process. After share verification for decryption with present two participants, by stacking share 1 and 2, secret image 1 appears and stacking share 1 on share 2 with 90 degrees rotation in clockwise help appear secret image 2.

Table I. Psnr Results

Image	PSNR	MSE
Secret image 1	9	7667
Secret image 2	11	5637

6. CONCLUSION

This paper presents a simple verifiable image secret sharing scheme using XOR Visual Cryptography. Proposed scheme can verify the share using steganography and then use XOR visual cryptography for share generation, by using this scheme preventing the misuse of adversaries. Cover image is shared by using the original shares created. Cover image is not making share size greater than secret image. Reconstructed cover image verifies the accuracy of reconstructed secret image. The proposed scheme is ideal, perfect, verifiable, reliable and secure.

7. REFERENCES

[1] G.R. Blakley, "Safeguarding cryptography keys," In Proceedings of AFIPS 1979 National Computer Conference,Volume. 48, pp.313-317,New York, USA, 1979.

[2] M. Noar, A. Shamir, "Visual cryptography," in: A. De Santis (Ed.),Advance in Cryptography: Eurpocrypt'94, Lecture Notes in Computer Science, Volume. 950, pp. 1-12, 1955.

[3] E. Verheul, H.V. Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," Designs, Codes and Cryptography, pp.179–196, 1997.

[4] D. Wang, L. Zhang, N. Ma, X. Li, "Two secret sharing schemes based on Boolean operations, "In Proceedings of Pattern Recognition. Published by Elsevier Science Ltd, pp. 2776-2785, 2007.

[5] C.C. Wu, L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[6] C. C. Chang, J. C. Chuang, Pei-Yu Lin , "Sharing A Secret Two-Tone Image In Two Gray-Level Images", Proceedings of the 11th International Conference on Parallel and Distributed Systems (ICPADS'05) , 2005.

[7] Duanhao Ou a , Wei Sun b,c,n , Xiaotian Wu ,"A Non expansible XOR based visual cryptography scheme with meaningful shares", 0165-1684 2014 Elsevier BV. All rights reserved.

[8] Rezvan Dastanian and Hadi Shahriar Shahhoseini ," Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares", 2011 International Conference on Information and Electronics Engineering IPCSIT vol.6 (2011) © (2011) IACSIT Press, Singapore

[9] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC 2008, IEICE, 2008.