2011 International Conference on Information and Electronics Engineering
IPCSIT vol.6 (2011) © (2011) IACSIT Press, Singapore

Multi Secret Sharing Scheme for Encrypting Two Secret Images into Two Shares

Rezvan Dastanian [1]and Hadi Shahriar Shahhoseini [2]

Electrical Engineering Department, Iran University of Science and Technology, Tehran, Iran
[1] r_dastanian@elec.iust.ac.ir [2] hshsh@iust.ac.ir

Abstract. Information, image and media encryption is a method for preventing misuse of adversaries. Because encryption and decryption normally need too complex computation. Visual cryptography is a method in witch decryption is performed with used via human visual system. In the traditional scheme; one secret image is divided between two shares so that by stacking the two shares secret image appears. One drawback of this scheme is the size of the shares is 4 times the size of the main secret image and transmission of the shares through internet needs too storage space and more bandwidth. In this paper a new visual cryptography scheme is proposed, that can transmit the two secret image with the use of two shares. With stacking two shares, secret image I appears and with stacking one of the shares with 90 degrees rotation in clockwise on other share appears the secret image II. The simulation results show properties of proposed scheme.

Keywords: Visual Cryptography, Halftone Technology, Multi Secret Sharing.

1. Introduction

With the rapid growth of computer networks and communication technologies, large amounts of digital data have been transmitted over the internet. However, secret data transmission over an open channel can be easily interfered, forged, or attacked by intruders. For the sake of security, secret data is often encrypted before transmission.

The concept of Secret Sharing Scheme (SSS) to solve the master key sharing problem was first introduced by Blakley and Shamir [1]. In order to protect the security of data, in 1994, Noar [2] proposed a new field of cryptography called Visual Cryptography (VC). Visual Cryptography Scheme (VCS) is a kind of secret sharing scheme which allows the encryption of a secret image into n shares that are distributed to n participants. The most important property of visual cryptography is that, the decryption of the secret images requires neither the knowledge of cryptography nor complex computation. The decoder is a human visual system and we can easily recover the secret by using the eyes of human being without the help of any computing devices.

The (k,n) threshold scheme is a scheme designed to divide the secret image to n different shares, so that the secret image is recoverable from any k (k<=n) shares and knowledge of k-1 or fewer shares provides absolutely no information about the secret image [3].

A SS scheme can be evaluated by its (a) security (b) reconstruction precision (contrast or accuracy), (c) computation complexity and (d) storage requirement (pixel expansion) [4]. The first criterion is satisfied if each share leaks no information from the original image and the original image cannot be reconstructed if there are fewer than k shares collected. The second criterion is considered to be the quality of the reconstructed secret image and evaluated by measuring the peak of signal-to-noise ratio. The computational complexity concerns the total number of operators required both to generate the set of n shadows and to reconstruct the original secret image. The last criterion, which affects data transmission speed, is also called the shadow size. A large shadow size implies high transmission and storage cost. An ideal VSS scheme must satisfy high security, high accuracy, low computational complexity, and small shadow size. All schemes must satisfy the security condition and most of the schemes can reconstruct the secret image accurately. The traditional non-visual SS scheme employs complex numerical computations, but Visual secret sharing (VSS) schemes utilize the human visual system for the reconstruction of the secret image and require little or no computation. One of the major drawbacks of the visual schemes is their 'pixel expansion' since each original pixel is coded into m subpixels per shadow images. The pixel expansion becomes so dramatically worse that forces overhead on the transmission bandwidth over the networks. In this paper, the proposed scheme can encode two secret images into two share images based on traditional (2,2) VSS.

The remaining part of this paper is organized as fallows. In section2, a brief description about current existing techniques in traditional VC is given. Section 3 introduces the proposed scheme in detail. The results of simulation of the proposed scheme are shown in section 4 and conclusion of this paper is stated in section 5.

2. Related works

VC that was proposed by Noar and Shamir [2] is (2,2) threshold VSS. In (2,2) threshold visual secret sharing, there are two transparencies, called shares. Both are noise-like as shown in Fig. 1 (b) and (c). Nobody can get secret image with on transparency. The probability of black pixel is 50%. By the stacking of the two transparencies, as shown in Fig.1 (b) and (c), the binary secret image will appear as Fig. 1 (d).

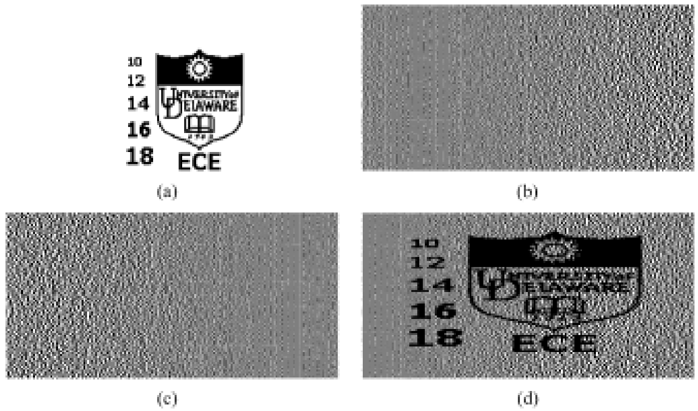


Fig. 1: (a) secret image, (b) share I, (c) share II, (d) the recovered image after stacking two shares

First the method to generate shares is predefined in the table as shown in Fig. 2 and then all pixels of original image are scanned.

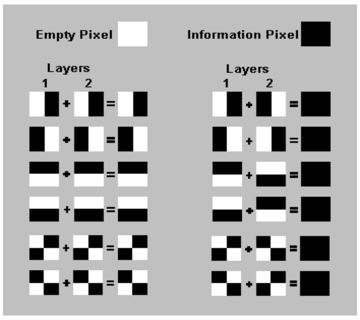


Fig. 2: Division of pixels in subpixels in Visual cryptography

In [5] Chen and Wu proposed a (2,2)-threshold visual secret sharing scheme for two secret images. The first secret image is decrypted by only stacking two share images. The second secret image is decrypted also by stacking two share images and one share image rotated. To overcome the angle restriction of Chen and Wu's scheme, Hsu et al [6] proposed another scheme to hide two secret images in two share images with arbitrary rotating angles. Their scheme rolls up the share images to become rings so that it becomes easy to rotate the share images at any desired angle. Feng and et al proposed the scheme to hide m secrets and to reveal the secrets by stacking the share images at m aliquot angles, respectively. Tzung-Her Chen et al [7] anticipated a multi-secrets visual cryptography which is extended from traditional VSS implemented to generate share images macro block by macro block in such a way that multiple secret images are turned into only two share images and decode all the secrets one by one by, stacking two of share images in a way of shifting. This scheme can be used for multiple binary, grey and colour secret images with pixel expansion of 4. Daoshun Wang et al [8] provided general construction for extended VC schemes using matrix extension algorithm. A general construction method for single or multiple and binary, greyscale, colour secret images using matrix extension utilizing meaningful shares was suggested. Using matrix extension algorithm any existing VCS with random-looking shares can be easily modified to utilize meaningful shares.

3. The proposed scheme

In order to share a A*A secret two-tone image between two participants, our system uses the two-out-of-two visual secret sharing technique to contruct two share, share1 and share2, of 2A*2A for sharing e secret two-tone image. Each secret bit is expanded to a block with 2*2 pixels. At first, based on halftone technology secret imams are transformed secret to binary images then dealer divides secret image1 to two shares, share a and share b, and secret image2 is also divided into two shares, share a', share b', based on the Noar's scheme.

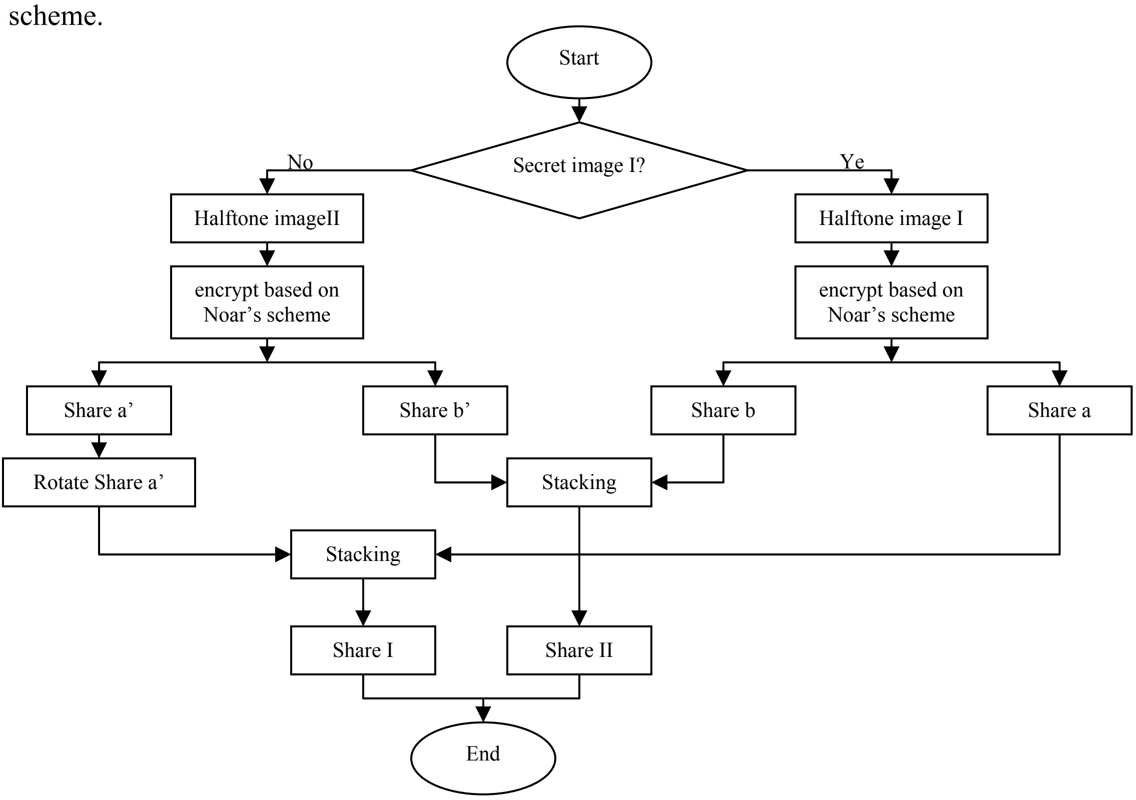


Fig. 3: Flowchart of the proposed scheme

As shown in Fig.3 flowchart of the proposed scheme, to make share A, dealer stacks share a' with 90 degrees rotation in counterclockwise on share a and for share B, share b stacking on share b'. Dealer distributes share A and B between two participants and for decryption with present two participants, by stacking share A and B, secret image I appears and stacking share A on share B with 90 degrees rotation in clockwise help appear secret image II.

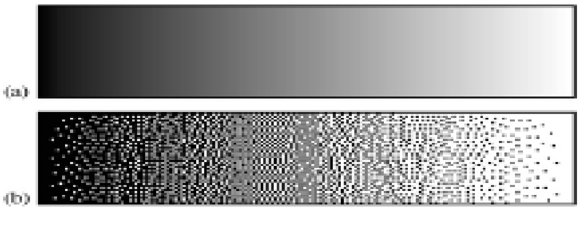
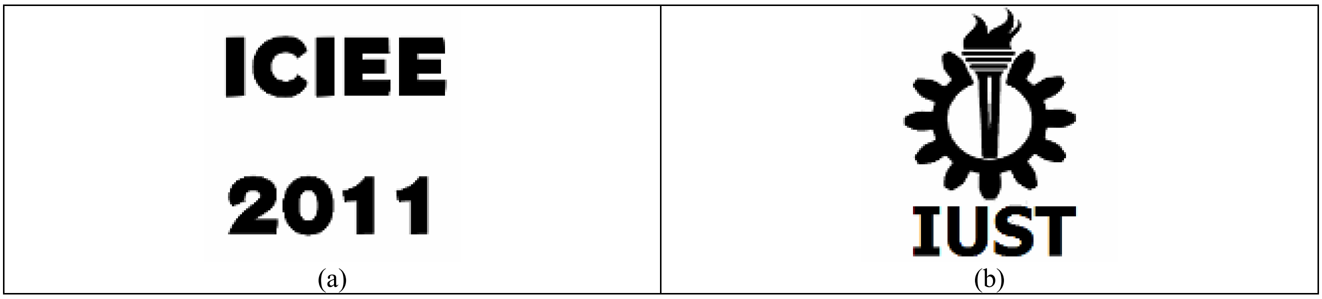


Fig. 4: (a) continuous tone, (b) halftone

The method that uses the density of the net dots to simulate the grey level is called 'halftone' and transforms an image with grey level into a binary image before processing [9]. For example, take the grey-level image in Fig. 4. Every pixel of the transformed halftone image has only two possible colour levels (black or white) as human eyes cannot identify too tiny printed dots, when viewing a dot, they tend to cover its nearby dots, we can simulate different grey levels through the density of printed dots, even though the transformed image actually has only two colours-black and white.

4. Simulation

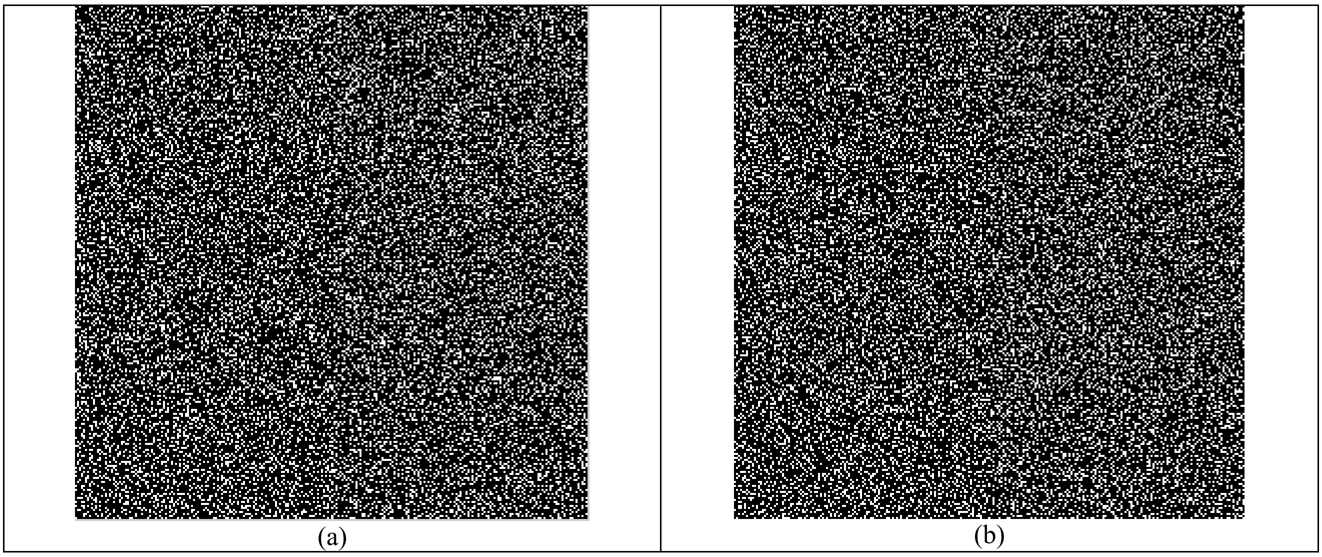
To show the efficiency of the proposed scheme we select two 128*128 pixels secret images shown in Fig. 5 (a) , (b).



(a) (b)

Fig. 5: (a) secret image I, (b) secret image II

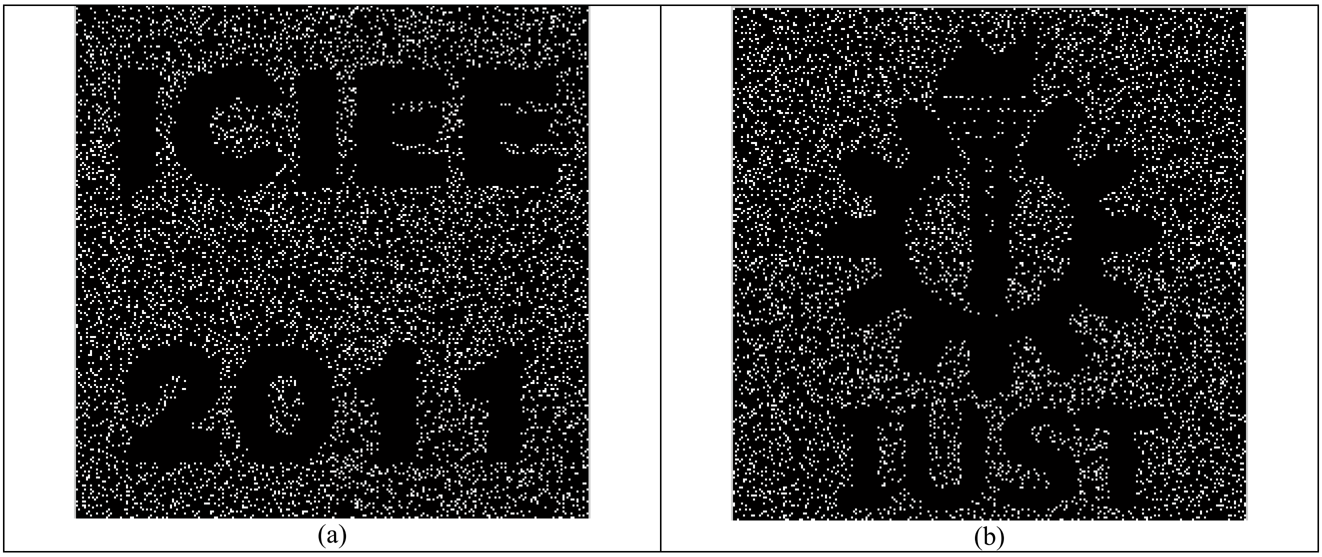
And by use of halftone technology the selected images are transformed to two binary images. Then binary image I is divided into two shares, share a , share b and binary image II into share a', b' with VCS's Noar. Then with stacking share a, share a' with 90 degrees rotation in counterclockwise make share A, and stacking share b and b' makes share B (Fig. 6 (a), (b))



(a) (b)

Fig. 6: (a) share I, (b) share II

For decryption it is sufficient to stack share A on share B that makes secret image I and for decryption of secret image II share A with 90 degrees rotation in clockwise stack on share B (Fig. 7 (a) , (b))



(a)

(b)

Fig. 7: (a) the recovered image I, (b) the recovered image II

5. Conclusion

One drawback of the traditional visual cryptography scheme proposed by Noar and Shamir, is; share's sizes are greater than the main secret image because each pixel of main secret image is transformed into one 4 pixels block in share images, so the transmission needs too storage space and more bandwidth and they encrypted only one secret image in themselves. In this paper one multi secret sharing for visual cryptography is proposed that can encrypt two secret images between two shares as with stacking two shares appear secret image I and with stacking one of shares with 90 degrees rotation on other share appear secret imageII.

Acknowledgment

The authors are thankful of the financial support provided by Iran Telecommunication Research Center (ITRC).

6. 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] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "Multi-Secrets Visual Secret Sharing", Proceedings of APCC2008, IEICE, 2008.

[8] D. Wang, F. Yi, X. Li, "On General Construction For Extended Visual Cryptography Schemes", Pattern Recognition 42 (2009), pp 3071 – 3082, 2009.

[9] R. Dastanian, H. S. Shahhoseini, "An Improved Visual Cryptography Scheme Using Scrambling Pixels in Color Images,' In Proceeding of ICCEI 2011, Volume. 1, pp. 80-84, China, 2011.