International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 4, August 2014, PP 46-52
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Secret Sharing Using Visual Cryptography

Renu Poriye
M.Tech. (C.SE)
Manav Rachna International University
Faridabad
renu.janagal@gmail.com

Dr S. S Tyagi
Head of Department
Department of Computer Engineering
Manav Rachna International University
Faridabad

Abstract: *Visual cryptography technique encipher the visual information in such a way, that decipher can be performed by human visual system without any complex process. Visual cryptography, is a secure process for transmitting visual information but, if anyone gets access to all shares, he/she can reveal out the secret easily. In this paper a visual cryptography scheme is proposed. This technique first encrypts the secret using a symmetric key and then divides the secret into shares. After piling of shares, secret does not appear, until the symmetric key is not known. This technique is proposed for binary images. Here the symmetric key used for encryption and decryption is a small binary image.*

Keywords: *Visual Cryptography, (key, 2, 2)Visual cryptographic scheme, Encryption*

1. Introduction

In order to guard data and debase computation, Naor and Shamir introduces the concept of Visual cryptography. Main feature of visual cryptography scheme (VCS) is that it does not need mathematical computation to get the original secret. In VCS [1][9], visual information is chopped into n shares and distributed to n participants. At least p no. of shareholders can reveal the actual image if their shares are piled properly in proper orientation. But fewer than p shares gets no information about the secret. This is referred as ‘p out of n’ VCS [2] and symbolically written as (p,n) VCS. The main problem of most visual cryptography scheme for binary image is that the decrypted image size is larger than original and also some security issues are present. The proposed VCS have tried to overcome both issue. The size of shares is same as original while security is provided using the concept of symmetric key encryption. We have also successfully implemented this scheme in Matlab R2009a. Here the proposed scheme is described in section-3. Result of implementation is shown in section-4. Comparison of new scheme with others is shown in section-5. Conclusion and Future work is described in section-6.

2. Related Work

Visual cryptography enrooted by M. Naor and A. Shamir, and they described general (p,n) VCS. When shares are merged using OR/XOR operation, grayed secret image recovered.

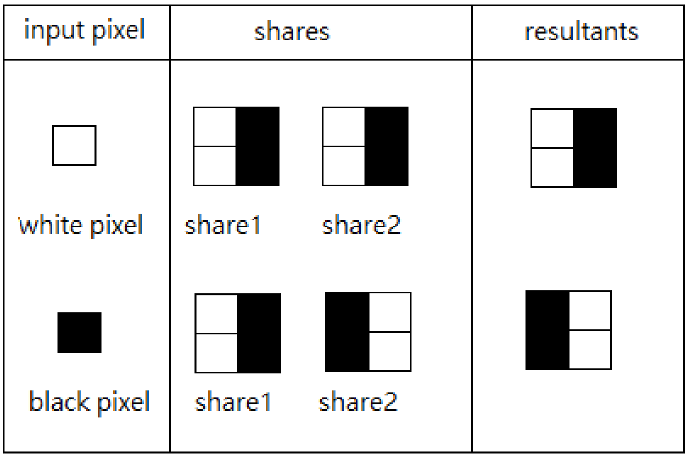

Fig1. *Shares used by Naor and Shamir in(2,2) VCS*

They designed (2,2) VCS using 4 subpixels, it means one pixel of original image provokes 4 subpixels in each share. Hence share size is 4 times as original. Here are some induced share for their (2,2) scheme[5][9] Tai-wen Yue and Chian[13] introduces a modified scheme in which the share dimension is twice of riginal in horizontal direction while remains same in vertical direction. Its contrast is same as Naor and Shamir 2 out of 2 schemes

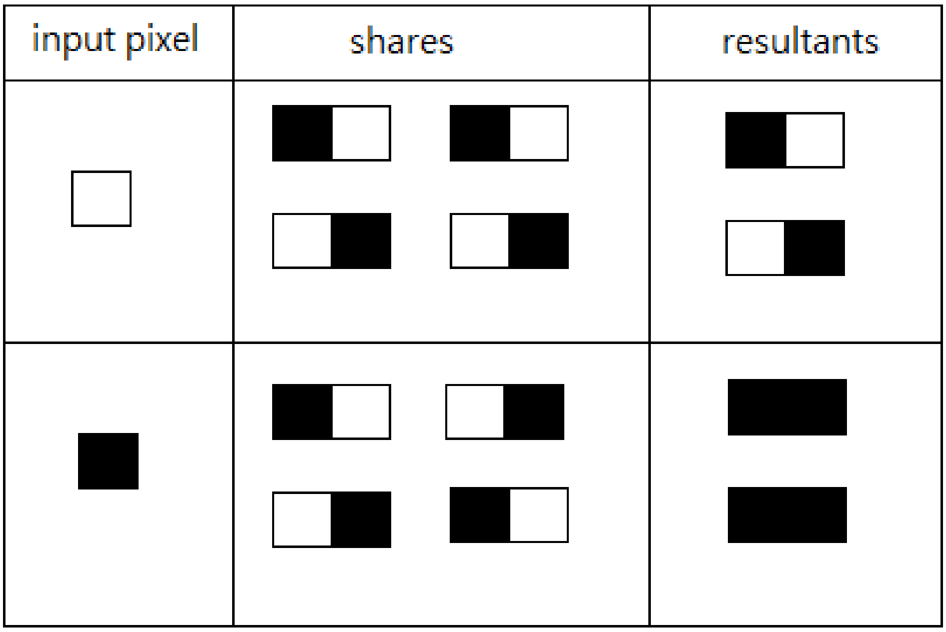

Fig2. *Shares used by Tai-wen and Suchen Chian[8]*

D. Jena and S. K. Jena proposed data hiding in halftone images using conjugate ordered dithering DHCOD)[5]. They considered security of shares [5] in visual cryptography. Firstly, shares are generated using basic scheme. Then these shares are watermarked [5] with some cover image using DHCOD [5]. The decryption is made by human visual system. Abhisek Parakh and Subhas Kak proposed a (2, 3) VCS based on recursive hiding scheme [1],[12].

All the above mentioned schemes increase the size of shares and loss visual fidelity.

3. The Scheme

The proposed scheme consider security of image in terms of encrypting it with the help of symmetric key, hence if someone access all the shares in unauthorized way, he/she cann't decrypt it completely without symmetric key. This scheme manages security as well as decrypted images are of same size as original. The scheme is divided into three parts:

- Encryption of original image using symmetric key.
- Generation of Shares
- Decryption of Overlapped shares.

3.1. Encryption Process

- Divide images into blocks such that block size equals to key size.
- Each block is XORed with key and then placed again in its original position.

Now, encrypted image is divided into shares using visual cryptography.

3.2. Share Generation

To overcome the increasing size problem, following approach is used for share generation. By considering 4 pixel of input image at a time and then generating 4 output pixel for each share[8].

There are 16 cases which are in following 5 Categories.

Shares and symmetric key is transmitted to the receiver. We can also divide the symmetric key into shares for more security.

Table1. *Cases for share generation*

Cases	original image	No. of ways	share1	share2
4 original pixels are white	□□ □□	1	□□ ■■	□□ ■■
4 original pixels are black	■■ ■■	1	■□ ■□	□■ □■
Any 2 pixels are black & 2 are white	■□ □■	6	□■ □■	□□ ■■
Any 3 pixels are white & rest is black	■□ □□	4	■□ □■	■□ □■
Any 3 pixels are black & rest is white	■■ ■□	4	□□ ■■	□■ □■

3.3. Decryption Process

At Receiver site, shares are combined and combined share is

- Divided into blocks such that block size equals to key size.
- Each block is XORed with key and then placed again in its original position.

Now original secret image is recovered.

4. Result

The above mentioned scheme is implemented into “MATLAB R2009a”. The results are as our expectation.

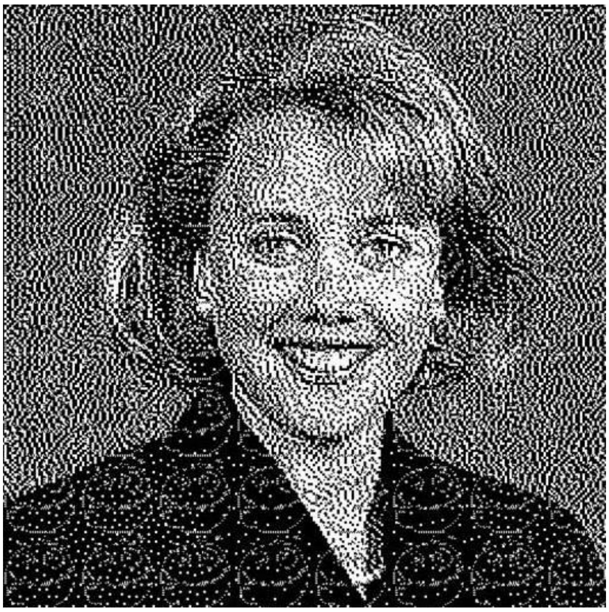

Fig3(a). *Original Secret Image (512 x 512)*

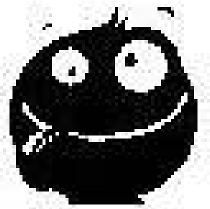

Fig3(b). *Key (64 x 64)*

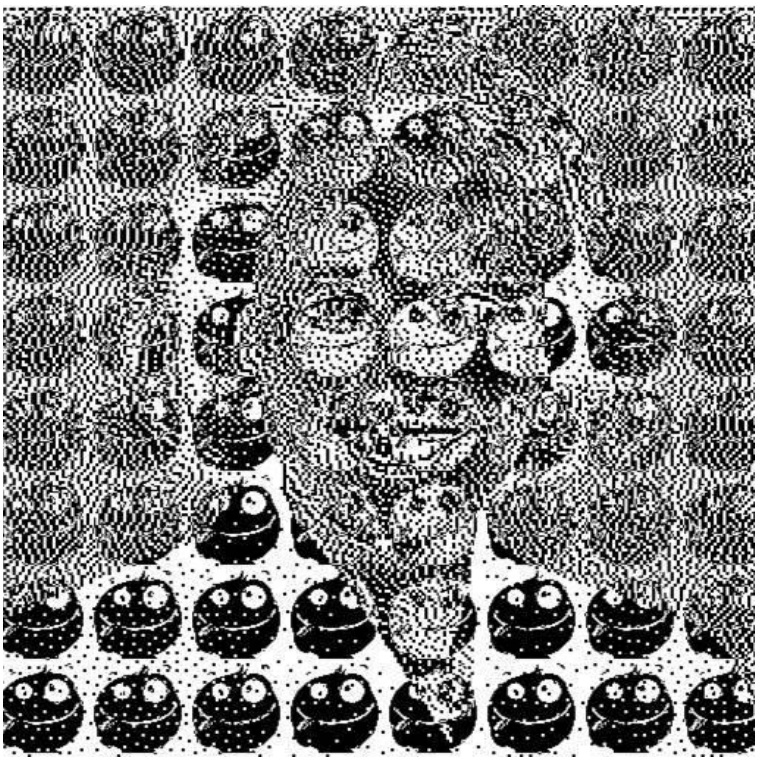

Fig3(c). *Encrypted Image (512 x 512)*

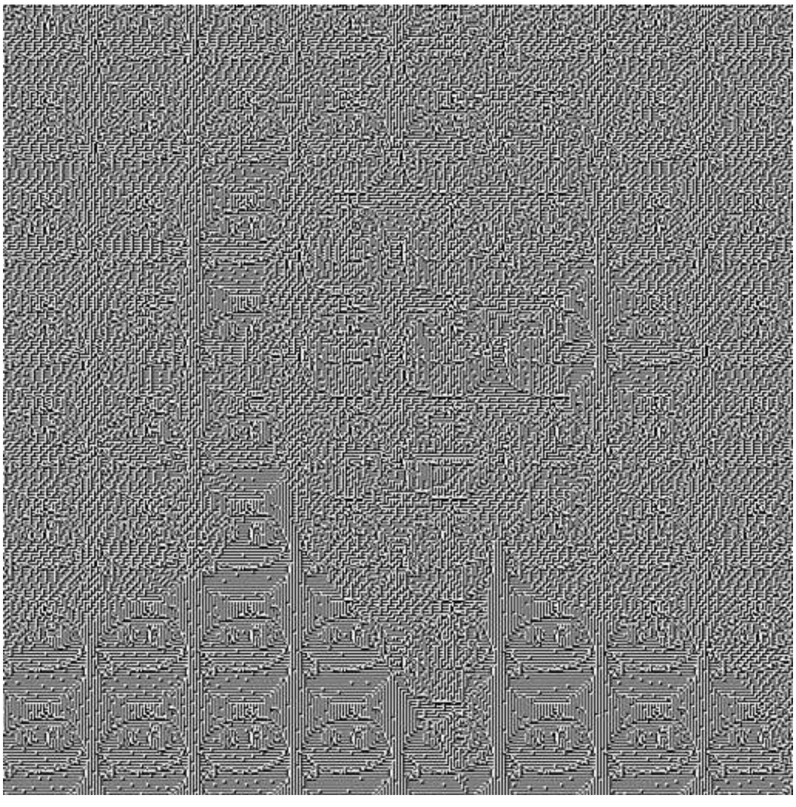

Fig3(d). *Share 1 (512 x 512)*

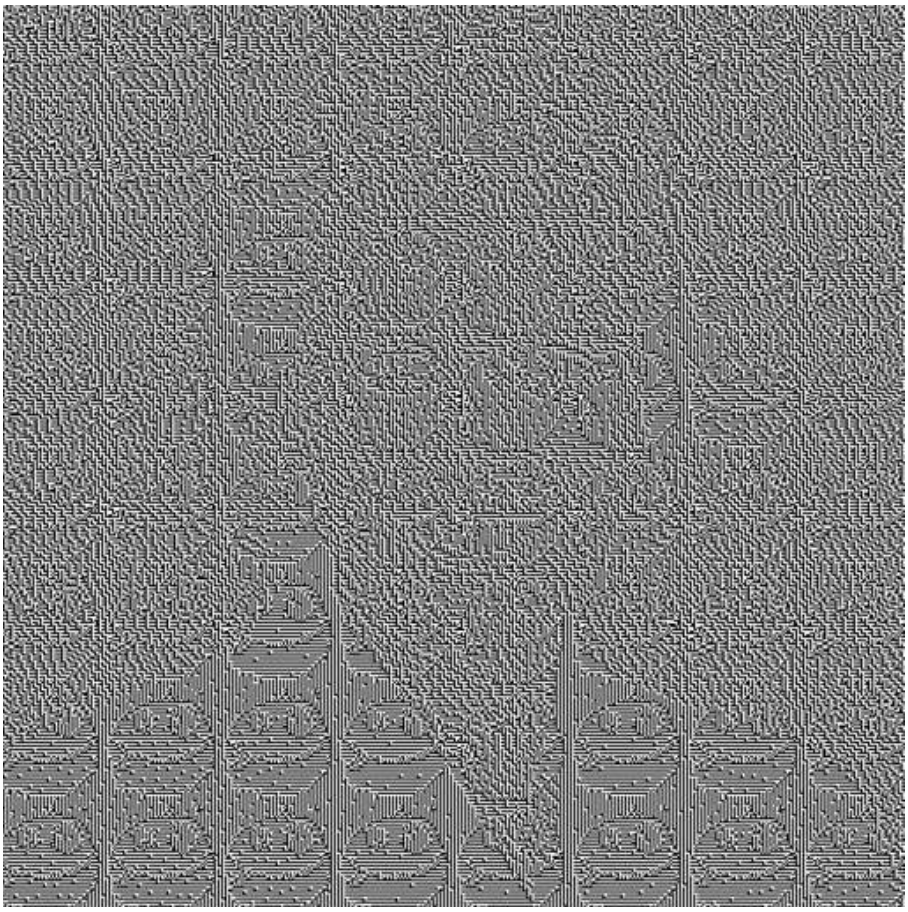

Fig3(e). *Share 2 (512 x 512)*

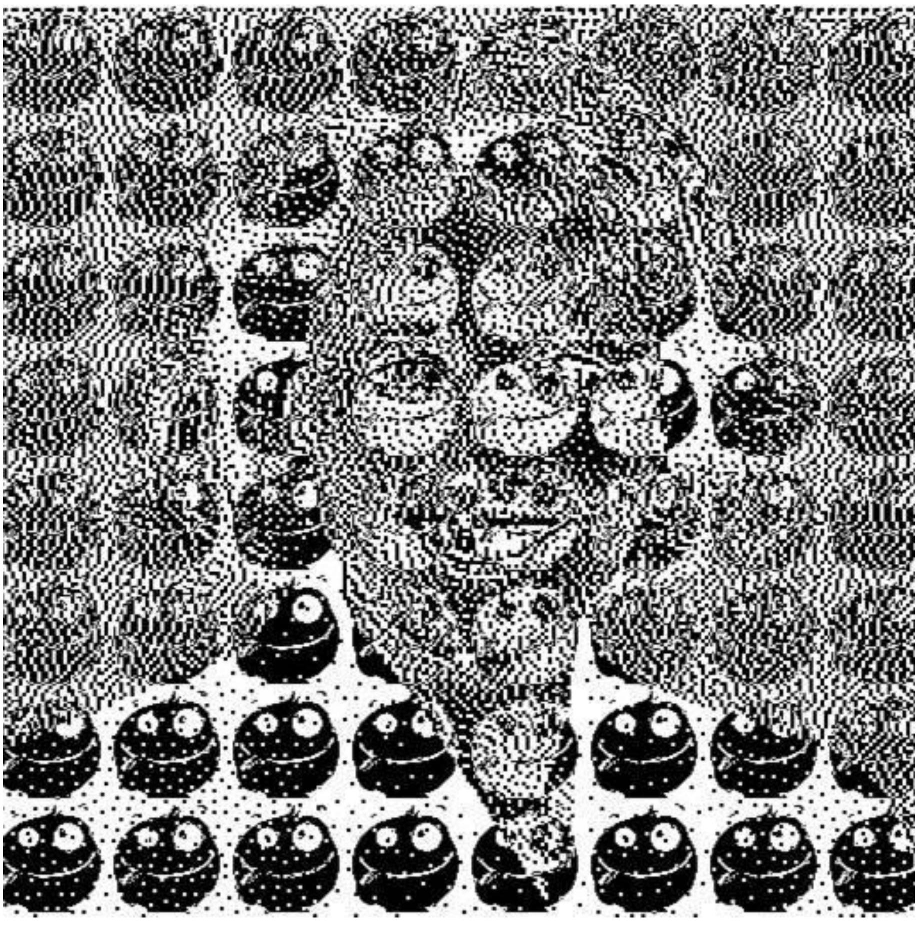

Fig3(f). *Overlapping Share 1 & Share 2 (512 x 512)*

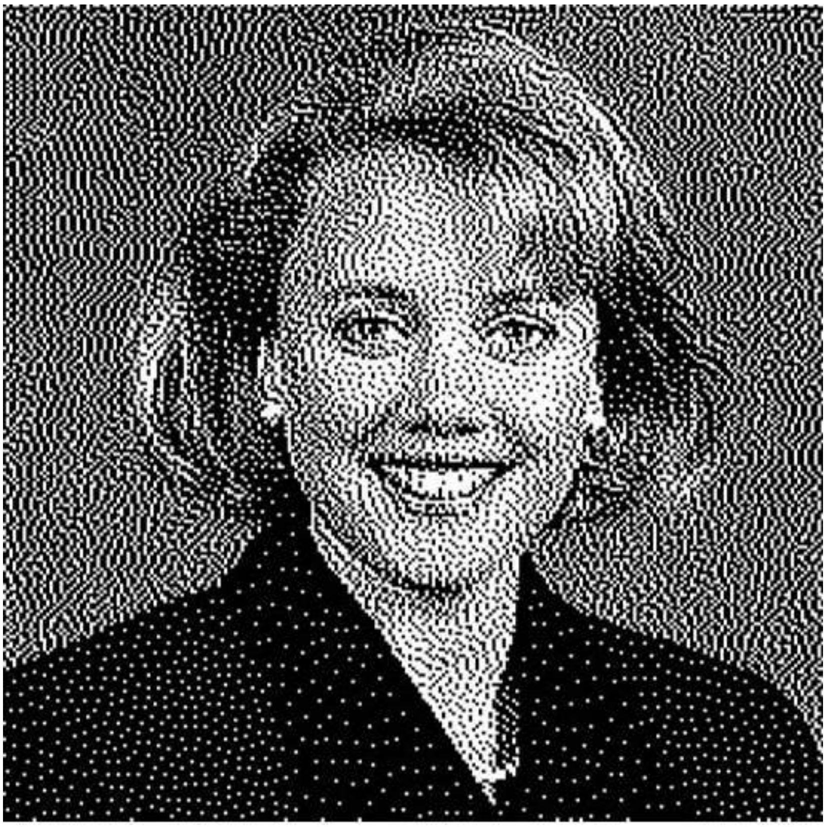

Fig3(g). *Decrypted Image (512 x 512)*

5. Comparison

The existing Visual Secret Sharing schemes increases size of decrypted image and security gets ruined if someone has access to all shares. The proposed scheme improves with respect to size and security with a limitation of aspect ratio of original image cannot be maintained.

Table2. *Comparison of proposed scheme with other vcs*

	Original Image	Each share of Naor and Shamir (2,2) Scheme	Each share of Basis (2,2) Scheme	Each Share of Proposed VCS
No. of Pixel	100	400	200	100
Security	Not Secure	Secure until all shares are not intercepts	Secure until all shares are not intercepts	More than all VCS until key is not known.

6. Conclusion & Future Work

As conclusion it can be said that; visual information where size and security is more concerned, the proposed visual cryptography scheme is undoubtedly fine and fantastic to use. But, this scheme increases some kind of computation at time of encryption and decryption. This scheme is best suitable for pictures having secret in the form of text. This scheme can be extended for colored images and for hiding multiple secrets. Instead of symmetric key, stream cipher can be applied for encrypting image.

Acknowledgements

We are thankful to technical staff of the Manav Rachna International University.

References

[1] Wu C., Chen L., A study on visual cryptography," Master's thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[2] Sirisha B. L., Lakshmi G. S., A novel cryptographic technique under visual secret sharing scheme for binary image, International Journal of Engineering Science and Technology, Vol. 2(5),2010, pp: 1473-1484.

[3] Yu B., Xu X., Fang L., Multi-secret Sharing Threshold Visual Cryptography Scheme, International Conference on Computational Intelligence and Security, 2007

[4] Parakh A., Kak S., A Recursive Threshold Visual Cryptography Scheme, Dept. of Computer Science, Oklahoma State University.

[5] Jena D., Jena S. K., A Novel Visual Cryptographic Scheme," IEEE,2008, pp. 207–211.

[6] Kessler G. C., An Overview of Cryptography"-

http://www.garykessler.net/library/crypto.html. 28 April 2013.

[7] Pal J. K., Mamdal J. K., Gupta K. D., A (2, N) Visual Cryptographic Technique For Banking Applications, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

[8] Weir J., Yan W. Q., Sharing Multiple Secrets Using Visual Cryptography, IEEE, 2009

[9] Naor M., Shamir A., Visual cryptography, Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science,1995,(950):pp. 1-12.

[10] Mandal, J.K.; Ghatak, S. A Novel Technique for Secret Communication through Optimal Shares Using Visual Cryptography (SCOSVC), Electronic System Design (ISED), 2011 International Symposium on, On page(s): 329 – 334

[11] Mandal, J.K.; Ghatak, S. Secret image / message transmission through meaningful shares using (2, 2) visual cryptography (SITMSVC), Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, On page(s): 263 – 268

[12] Katta S., Recursive Information Hiding in Visual Cryptography, 2010

[13] Yue T. W., Chiang S., A Neural Network Approach for Visual Cryptography. Proceedings of the IEE-INNS-ENNS International Joint Conference on Neural Networks(IJCNN'00) .pp. 1-2.

[14] Chakraborty U., Paul J. K., Mahapatra P. R. S., "Desigan and Implementaion of a (2,2) and a (2,3) Visual cryptographic scheme". IJCCT Vol.1 Issue 2,3,4; 2010 .