I. J. Computer Network and Information Security, **2019, 11, 14-20**
Published Online November 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.11.02

An Efficient (n, n) Visual Secret Image Sharing using Random Grids with XOR Recovery

Ram Gopal Sharma
Research Scholar, Uttarakhand Technical University, Dehradun, India
E-mail: cs.ramgopal@gmail.com

Dr. Hitendra Garg and Dr. Priti Dimri
GLA University, Mathura, India
G. B. Pant Engineering College, Ghurdauri, Pauri
E-mail: hitendra.garg@gmail.com, pdimri1@gmail.com

Received: 26 July 2019; Accepted: 11 September 2019; Published: 08 November 2019

Abstract—Visual cryptography by name itself suggests cryptography related to images. It is a branch of cryptography that deals with the encryption and decryption of images. Visual cryptography demonstrates a visual secret sharing scheme in which an image has been divided into n shares and original image can be decrypt with these shares without / less computational efforts. This paper proposed an efficient (n, n) visual secret image sharing method using random grids. This scheme gives the complete retrieval of secret image using XOR stacking without the need of a codebook. The Random Grid based Visual Cryptography results no pixel expansion. The proposed method works for $n \geq 3$ (shares) for retrieval of original image. Experimental results demonstrate that the proposed method produces better results in terms of simplicity, visual quality and performance.

Index Terms—Visual Secret Image Sharing, Visual Cryptography, Contrast, Random grids.

I. Introduction

Visual Cryptography Scheme (VCS) is a method of Visual Secret Sharing (VSS) suggested by Naor and Shamir that suggest the retrieval of image by stacking the share of the image without any cryptographic computational efforts [1]. In VCS, an original image is encrypted into different images called shares.VSS schemes require *k*-out-of-*n* shares to get the original image. Each share (Random binary pattern) has been distributed among 'n' participants. Single share cannot retrieve complete information about original image, at least k-out-of-n (k is subset of n) shares are needed. Using human visual system (HVS), we can easily retrieve the original image with the stacking of these shares together, without any computation and cryptographic knowledge. This process is called VCS with OR stacking. In this type of method, we can retrieve not more than 50 % visual quality. To measure the visual quality of the retrieve image, we calculate the contrast of the image. We discussed the contrast calculation in section IV. We can also retrieve the secret image with XOR stacking. In this approach, we use XOR operator for stacking to produce retrieve the original image with high visual quality. Traditional VCS reports the pixel expansions i.e. shares generated are more in size than the actual image. VCS produces both meaningful and random (non-meaningful) shares.

G. Ateniese et al. developed a threshold k-out-of-n VCS method [2]. The technique proposed by G. Ateniese et al. [2] reports better results than the scheme suggested by Naor and Shamir [1] with less pixel expansion. Ito's et al. [3] removes the problem of pixel expansion in their research i.e. retrieve image after stacking and original image both are equal in size.

VSS by random grids (RG) removes the pixel expansion problem and there is no requirement of codebook design. Kafri and Keren [4] proposed the overview of RG. It is 2D array consists of pixels. With the use of coin flip method, we got every pixel, either fully transparent or opaque in a random manner. The transparent pixel (white) passes the light and opaque pixels (black) stop the light. The numbers of transparent pixels and opaque pixels are same in random grid [5] probabilistically. Table 1. presents the results after superimposing of the two random pixels k_1 & k_2. According to their scheme the secret image is encrypted into two meaningless RG.

Table 1. Results after superimposing of two random pixels

k_1	k_2	$k_1 \otimes k_2$
0	0	0
0	1	1
1	0	1
1	1	1

The proposed paper suggests a new approach for threshold n out of n VCS using Random Grid with XOR operator for stacking at recovery end. This paper gives the novel approach for VSS using random grid with XOR recovery. The proposed method recovers the information completely using XOR operator for stacking without pixel expansion. The proposed method does not require any code book and also not support pixel expansion (secret image and shares are equal in size). Table 2. & Table 3. give the abbreviations and notations used in this proposed paper respectively.

This paper is arranged as follows: Sections II discusses the literature review and concept of Visual Secret Sharing (VSS) using random grids. Section III defines the proposed method. Section IV defines the performance analysis. The different experimental results are discussed in section V. In the end, Section VI concludes the proposed technique.

Table 2. Notations used in this paper

SNo	Notations	Descriptions
1	1(resp. 0)	A Black(resp. White) pixel
2	$I_1, I_2 \ldots\ldots\ldots I_n$	Shares generated
3	$\otimes$	OR operation for stacking
4	$\oplus$	XOR operation for stacking
5	I	Original Secret Image
6	I_S	Secret Image after stacking

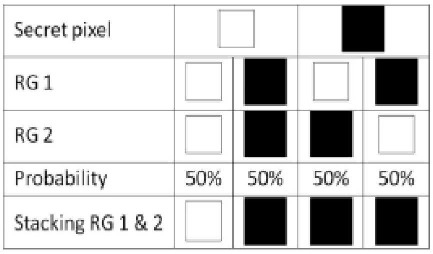
Table 3. Abbreviations used in this paper

SNo	Abbreviations	Descriptions
1	VCS	Visual Cryptography Scheme
2	VSS	Visual secret image sharing
3	HVS	Human Visual System
4	RG	Random Grid
5	PVCS	Progressive VCS

II. Literature Review

Encryption of secret image (binary) based on RG was first proposed by Kafri and Karen [4]. They proposed three algorithms for encrypting the image into RGs. The principle of one of the algorithm is described in Fig.1. A secret pixel is taken from the secret binary image and is encrypted into the subpixels in each of the two RGs. The subpixels are selected randomly form the two columns under the certain secret pixel. There is the random selection so that each column is selected with 50% probabilities. In that fashion the first sub pixel is assigned to RG1 and the followed up pixel is assigned to RG2 this process follows up till the last pixel of the secret image. So it confirmed that individual share cannot give any clue about the secret image. When we stack these shares the black pixels will cover the white pixels, and the white pixel will decode into the black or white pixel with 50% probabilities. This scheme is known as RG-based (2, 2) VC. The size of the shares is same as that of the secret image. There is some loss of contrast in the revealed image but we can clearly identify the image.

S. J. Shyu [6] further extend their work proposed in [5] for encrypting the image with multiple RG. This is a method of image encryption using the visual cryptograms of $n \geq 2$. Chen and Tsao [8] developed a User-friendly VSS based on RG. In this method, they produce meaningful shares using cover image without the pixel expansion. They analyze their method with the method developed in [7] in terms of share type, contrast, pixel expansion and image format etc.



Secret pixel	□		■	
RG 1	□	■	□	■
RG 2	□	■	■	□
Probability	50%	50%	50%	50%
Stacking RG 1 & 2	□	■	■	■

Fig.1. RG based 2 out of 2 Visual Cryptography Scheme

In (k, n) threshold VSS, we require only k shares to retrieve the secret image. T. H. Chen and K. H. Tsao [9] proposed a new threshold (k, n) VSS using RG for color and binary images. The developed method gives good visual quality and security. We cannot reveal image with less than k shares.

To construct meaningful shares in VSS, we use a cover image to encrypt the secret image. This concept is used by Wu, X. et. al [10] and produce meaningful shares. They use XOR stacking to retrieve secret image. To improve the contrast and use void & cluster based post processing mechanism in the work proposed by Wu, X. & Sun, W. [11,12] use the generalized RG to adjust the light transmission of a share.

Y. C. Hou et al. [13] developed a method based on RG in which they produce random and meaningful shares using different cover images. This method gives good result as compared to the method proposed by Chen and Tsao [8]. Yang, C. N. et al [14] investigates the relation between OR based VCS and XOR based VCS. Y. C. Hou et al. [15] developed a novel scheme that allows different privileges to different participants.

There are two methods for stacking the shares to retrieve the original image. One is OR based and other XOR based stacking. Using XOR we get better visual quality. Duanhao Ou et al. [16] developed a XOR based (n, n) VCS and produce meaningful shares.

Xuehu Yan et al. [17] proposed threshold (k, n) VCS with multiple decryption method such as OR and XOR based stacking. We can also apply this method for color images or grayscale images. Yan, X. et al [18] developed a RG based VSS and use OR and XOR decryption method.

Xuehu Yan et al. [19] proposed a novel threshold VSS based on RG which progressively increased the visual quality. With increasing the stacked shares, the visual quality of retrieve image is also increased. This method is known as Progressive VCS (PVCS).Pei-Ling Chiu et al. [20] developed a user friendly PVCS using XOR and produce meaningful shares.

Her-Chang Chao et al. [21] also proposed a RG based PVCS with XOR ability. Yan, X. et al [22] analyze the visual quality and difference between related methods and proposed new threshold VSS scheme using RG.

VSS can be applied in many areas of research, authentication, and security of information. In this paper, we developed (n, n) VSS based on RG using XOR to retrieve 100% visual quality of original image.

Table 4. gives the performance measures of different VSS discussed in [23]. This table gives the comparative study of different VSS based on different parameter such as pixel expansion, decryption method and type of VSS. This study helps to choose secure and suitable method for particular problem base on different parameters.

Table 4. Performance measures of various VSS

SNo.	Schemes	Pixel Expansion	Meaningful Shares	Decryption Method	Type of VSS
1	Ours	No	No	XOR	n out of n (n>=3)
2	[1]	Yes	No	OR	k out of n
3	[2]	Yes	No	OR	n out of n k out of n
4	[4]	No	No	OR	2 out of 2
5	[5]	No	No	OR	2 out of 2
6	[6]	No	No	OR	n out of n
7	[7]	No	Yes	OR	2 out of 2
8	[8]	No	Yes	OR	2 out of 2
9	[9]	No	No	OR	k out of n
10	[12]	Yes	No	XOR	n out of n
11	[13]	No	Yes	OR	2 out of 2
12	[14]	No	No	OR	k out of n
13	[16]	No	Yes	XOR	n out of n
14	[17]	No	No	OR, XOR	k out of n
15	[19]	No	No	OR	k out of n
16	[20]	No	Yes	XOR	2 out of n
17	[21]	No	No	XOR	2 out of n

III. PROPOSED METHOD

In the proposed method, input is image (Binary). The size of image is A × B. First we generate n-1 shares using random grid, then generate share n by the proposed algorithm 1. For decryption, use algorithm 2. Diagram for share generation is shown in Fig.2.

There are eight steps to generate n shares for n out of n secret image sharing in proposed method. We take a secret image (I) of size A ×B and create n-1 shares in random way i.e. put random pixels in I_1, I_2, I_3……………… I_{n-1} using step 1 and 2. For nth share, we use step 4 to 8 of algorithm 1. We generate a matrix X of size A ×B using step 4then we calculate the pixel (i, j) of nth share using X and the original secret image I using step 5 to 8. In this way we create all n shares. Using algorithm 2, we simply reconstruct the secret image I_S completely without loss of information.

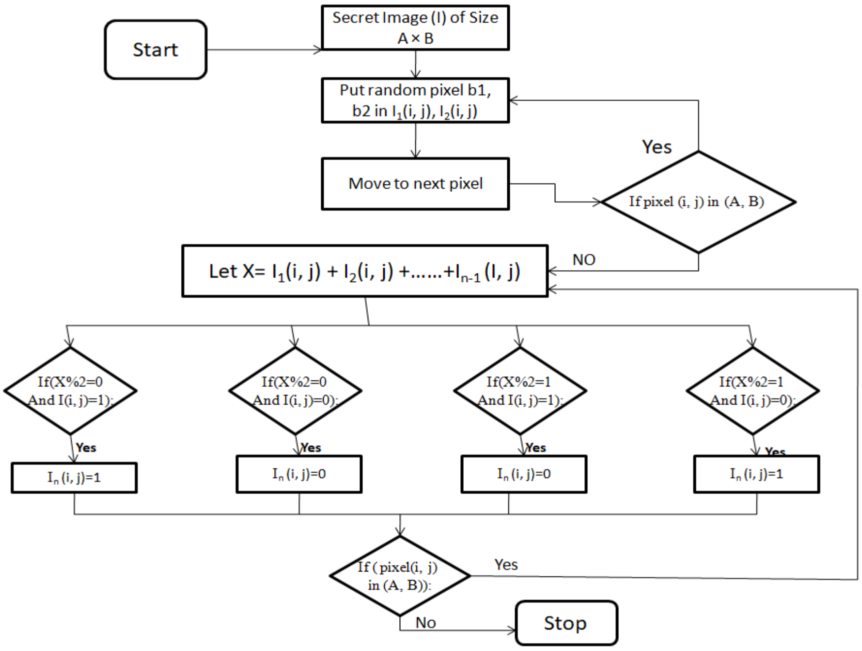


Fig.2. Share generation procedure of XOR based (n, n) VSS using random grid

Algorithm 1: For Encryption

```
Input: A ×B binary image (Secret image) I
Output: n shares $I_1, I_2 .................I_n$
1: For every position (i,j) $\in \{(i,j) | 1 \le i \le A; 1 \le j \le B\}$ repeat step 2
2: Put random pixel $b_1, b_2, b_3 .................b_{n-1}$ in $I_1(i,j), I_2(i,j) .................I_{n-1}(i,j)$
3: For every position (i,j) $\in \{(i,j) | 1 \le i \le A; 1 \le j \le B\}$ rep eat step 4-8
4: Let $X = I_1(i,j), I_2(i,j) .................I_{n-1}(i,j)$
5: if X%2=0 and I(i,j)=1 then In(i,j)=1
6: if X%2=0 and I(i,j)=0 then In(i,j)=0
7: if X%2=1 and I(i,j)=1 then In(i,j)=0
8: if X%2=1 and I(i,j)=0 then In(i,j)=1
```

Algorithm 2: For Decryption

```
Input: n shadow images I1,I2,.........In
Output: A ×B binary secret image I

1: For every position (i,j) $\in \{(i,j) | 1 \le i \le A; 1 \le j \le B\}$ repeat step 2
2: $I_s = I_1(i,j) \oplus I_2(i,j) \oplus I_3(i,j) ................ \oplus I_n(i,j)$
3: Secret image I
```

IV. Performance Analysis

Definition 1 (Contrast): An important measure of VCS is contrast of the reconstructed image i.e. visibility of the secret image. We can calculate the Contrast (α) of the retrieve image using

$$\alpha = (A_0 - A_1) / (1 + A_1) \tag{1}$$

Where A_0 = Probability of correctly decrypted Zero's of the original secret image A_1= Probability of wrongly decrypted the One's of original secret image

Definition 2 (Security): Security condition means that we can retrieve original image with insufficient shares.

Proof: According to step 2, the shared pixel is independent of the secret pixel; no matter the secret image is 0 or 1. Only n^{th} share is dependent on secret image in step 4 to 8 but it is insufficient to retrieve image with only n^{th} share. So, each share has no clue about secret image.

Definition 3 (Visually recognizable): The retrieve image I_s is recognizable as original image by α >0. If α =1, then the image is fully retrieved.

V. Results

The proposed method results show the 100% recovery of the image after stacking the shares. Fig.3. shows the experimental result of (3, 3) threshold VSS on binary image Baboon: 512* 512 pixels using proposed method. The contrast of Fig.3 (e) is 1. Fig.4. shows the experimental result of (4, 4) threshold VSS on binary image Baboon: 512* 512 pixels using proposed method. The contrast of Fig.4 (f) is 1. Fig.5. shows the experimental result of (5, 5) threshold VSS on binary image Baboon: 512* 512 pixels using proposed method. The contrast of Fig.5 (g) is 1. Fig.6. shows the experimental result of (3, 3) threshold VSS on binary image Lena: 512* 512 pixels using proposed method. The contrast of Fig.6 (e) is 1. Fig.7. shows the experimental result of (4, 4) threshold VSS on binary image Lena: 512* 512 pixels using proposed method. The contrast of Fig.7 (f) is 1. Fig.8. shows the experimental result of (5, 5) threshold VSS on binary image Lena: 512* 512 pixels using proposed method. The contrast of Fig.8 (g) is 1.

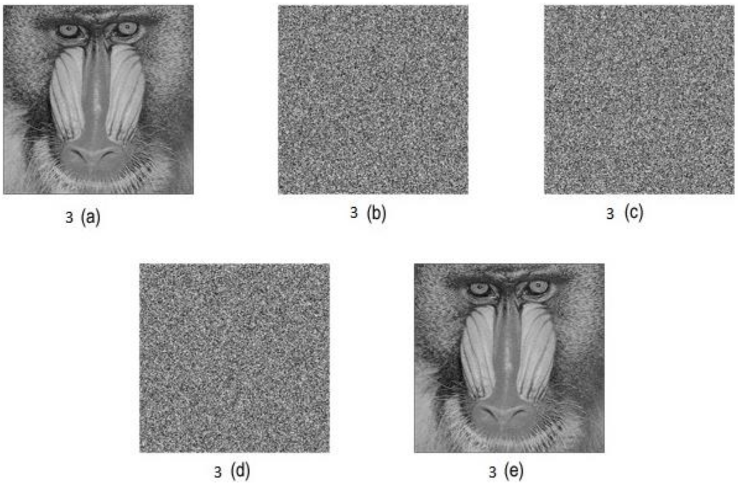


Fig.3. The experimental result of (3, 3) threshold VSS. 3(a): baboon image, 3(b)-(d): Shares 1-3, 3(e): Image after stacking using XOR.

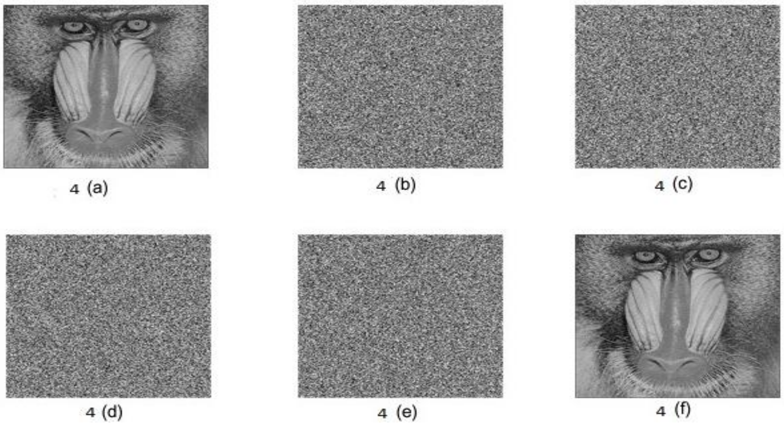


Fig.4. The experimental result of (4, 4) threshold VSS on binary image Baboon: 512* 512 pixels using proposed method. 4(a): Baboon image, 4(b)-(e): Shares 1-4, 4(f): Image after stacking using XOR

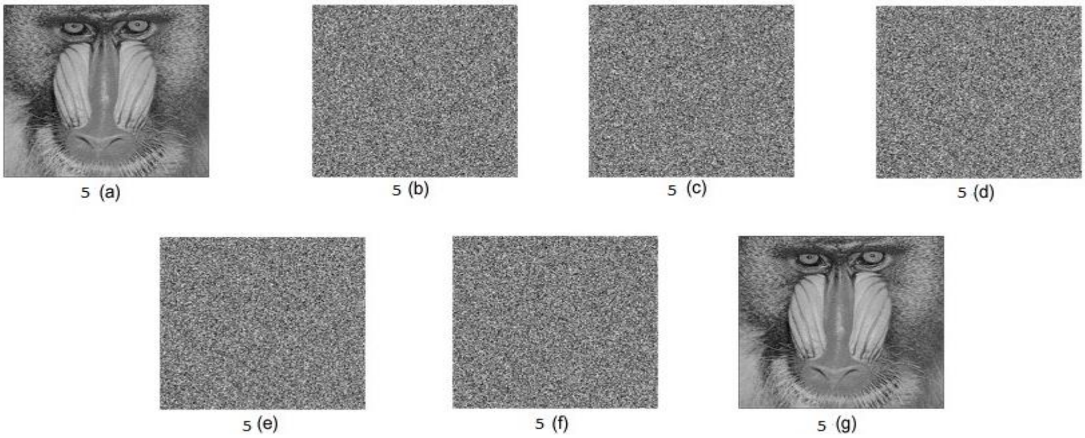


Fig.5. The experimental result of (5, 5) threshold VSS on binary image Baboon: 512* 512 pixels using proposed method. 5(a): Baboon image, 5(b)-(f): Shares 1-5, 5(g): Image after stacking using XOR.

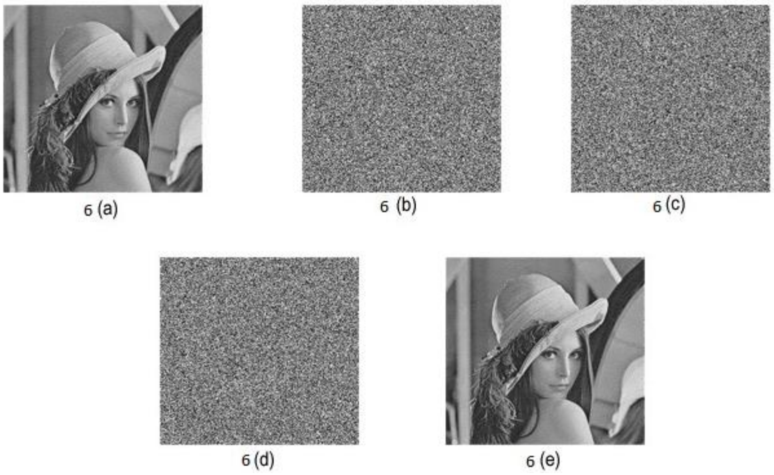


Fig.6. The experimental result of (3, 3) threshold VSS on binary image Lena: 512* 512 pixels using proposed method. 6(a): Lena image, 6(b)-(d): Shares 1-3, 6(e): Image after stacking using XOR.

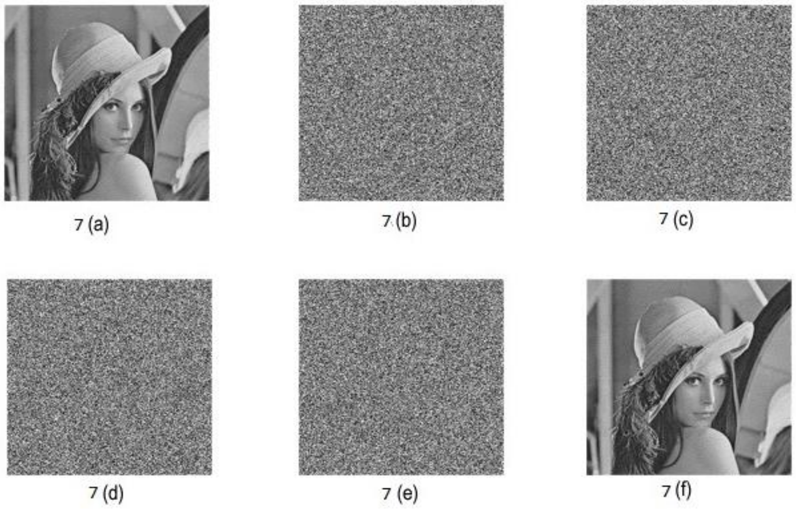


Fig.7. The experimental result of (4, 4) threshold VSS on binary image Lena: 512* 512 pixels using proposed method. 7(a): Lena image, 7(b)-(e): Shares 1-4, 7(f): Image after stacking using XOR.

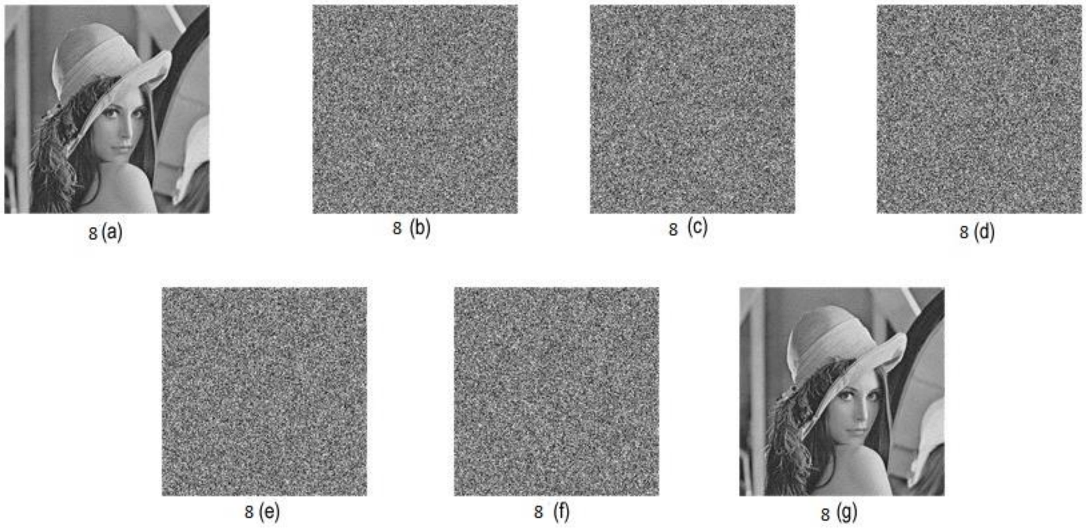


Fig.8. The experimental result of (5, 5) threshold VSS on binary image Lena: 512* 512 pixels using proposed method. 8(a): Lena image, 8 (b)-(f):Shares1-5, 8(g): Image after stacking using XOR.

VI. Conclusion

For data (Image) transmission over the internet, we have to be considering the security and simplicity aspect. One method is data encryption. Another way is visual secret sharing schemes, these are easy in implementing and at the receiver end, and we have no need of computation for decryption process. This paper gives a new approach of (n, n) visual secret image sharing method using random grid based on XOR recovery. Table 4. gives the comparative study of different VSS with our method to show the performance measure. Section 5 describes the contrast, security, visual recognizable definition and proof to show this method is easy to implement, secure and good visual quality without pixel expansion. Experimental results are shown that this method is easy to implement and we retrieve the secret image completely without loss of information. To improve the visual quality of retrieve image in case of meaningful shares will be the future work.

References

[1] Naor, M., & Shamir, A. (1995). Visual cryptography. Advances in Cryptology EUROCRYPT'94 Lecture Notes in Computer Science. In *Workshop on the Theory and Application of Cryptographic Techniques, May 9C12* (pp. 1-12).

[2] Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (1996). Visual cryptography for general access structures. *Information and Computation*, *129*(2), 86-106.

[3] Ito, R., Kuwakado, H., & Tanaka, H. (1999). Image size invariant visual cryptography. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, *82*(10), 2172-2177.

[4] Kafri, O., & Keren, E. (1987). Encryption of pictures and shapes by random grids. *Optics letters*, *12*(6), 377-379.

[5] Shyu, S. J. (2007). Image encryption by random grids. *Pattern Recognition*, *40*(3), 1014-1031.

[6] Shyu, S. J. (2009). Image encryption by multiple random grids. *Pattern Recognition*, *42*(7), 1582-1596.

[7] Chen, T. H., Tsao, K. H., & Yang, Y. T. (2009). Friendly color visual secret sharing by random grids. *Fundamenta Informaticae*, *96*(1-2), 61-70.

[8] Chen, T. H., & Tsao, K. H. (2011). User-friendly random-grid-based visual secret sharing. *IEEE Transactions on Circuits and Systems for Video Technology*, *21*(11), 1693-1703.

[9] Chen, T. H., & Tsao, K. H. (2011). Threshold visual secret sharing by random grids. *Journal of Systems and Software*, *84*(7), 1197-1208.

[10] Wu, X., Ou, D., Dai, L., & Sun, W. (2013, June). XOR-based meaningful visual secret sharing by generalized random grids. In *Proceedings of the first ACM workshop on Information hiding and multimedia security* (pp. 181-190). ACM.

[11] Wu, X., & Sun, W. (2013). Improving the visual quality of random grid-based visual secret sharing. *Signal Processing*, *93*(5), 977-995.

[12] Wu, X., & Sun, W. (2013). Generalized random grid and its applications in visual cryptography. *IEEE Transactions on Information Forensics and Security*, *8*(9), 1541-1553.

[13] Hou, Y. C., Wei, S. C., & Lin, C. Y. (2014). Random-grid-based visual cryptography schemes. *IEEE Trans. Circuits Syst. Video Techn.*, *24*(5), 733-744.

[14] Yang, C. N., & Wang, D. S. (2014). Property analysis of XOR-based visual cryptography. *IEEE transactions on circuits and systems for video technology*, *24*(2), 189-197.

[15] Hou, Y. C., Quan, Z. Y., & Tsai, C. F. (2015). A privilege-based visual secret sharing model. *Journal of Visual Communication and Image Representation*, *33*, 358-367.

[16] Ou, D., Sun, W., & Wu, X. (2015). Non-expansible XOR-based visual cryptography scheme with meaningful shares. *Signal Processing*, *108*, 604-621.

[17] Yan, X., Wang, S., Niu, X., & Yang, C. N. (2015). Random grid-based visual secret sharing with multiple decryptions. *Journal of Visual Communication and Image Representation*, *26*, 94-104.

[18] Yan, X., Wang, S., El-Latif, A. A. A., & Niu, X. (2015). Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery. *Multimedia Tools and Applications*, *74*(9), 3231-3252.

[19] Yan, X., Lu, Y., Huang, H., Liu, L., & Wan, S. (2016, August). Quality-adaptive threshold visual secret sharing by random grids. In *Signal and Image Processing (ICSIP), IEEE International Conference on* (pp. 323-327). IEEE.

[20] Chiu, P. L., & Lee, K. H. (2016, October). An XOR-based progressive visual cryptography with meaningful shares. In *Computer Communication and the Internet (ICCCI), 2016 IEEE International Conference on* (pp. 362-365). IEEE.

[21] Chao, H. C., & Fan, T. Y. (2017). XOR-based progressive visual secret sharing using generalized random grids. *Displays*, *49*, 6-15.

[22] Yan, X., Liu, X., & Yang, C. N. (2018). An enhanced threshold visual secret sharing based on random grids. *Journal of real-time image processing*, *14*(1), 61-73.

[23] Sharma, R. G., Dimri, P., & Garg, H. (2018). Visual cryptographic techniques for secret image sharing: a review. *Information Security Journal: A Global Perspective*, *27*(5-6), 241-259.

Authors' Profiles

Ram Gopal Sharma received B.Tech in 2004 and M.Tech in 2013. He has thirteen years of teaching experience.

Presently, He is pursuing Ph.D. at Uttarakhand Technical University, Dehradun. He is presently working as an Assistant Professor in the department of Computer Science & Engineering of RBS Engineering Technical Campus, Bichpuri, Agra, India.

Dr. Hitendra Garg did his PhD (CSE) from Motilal Nehru National Institute of Technology, Allahabad and Masters (Software Systems) from BITS-Pilani.

He is presently working as Associate Professor in Department of Computer Engineering and Applications of GLA University, Mathura, India. He has total experience of more than 17 years in the field of academics / research. He has more than 20 research papers in the international journals / conference of repute. His research areas are Image Processing, Visual Cryptography, 3D data processing.

Dr. Priti Dimri received the MCA from the Gurukul Kangri University, MBA from Sikkim Manipal University and Ph.D. degree from Uttarakhand Technical University, Dehradun.

Currently, She is serving as an Associate Professor, Department of Computer Science and Applications, G. B. Pant Engineering College, Ghurdauri, Pauri. She has published many research papers in reputed journal and international conferences. She has delivered many expert lectures and keynote addresses in national and international conferences.

How to cite this paper: Ram Gopal Sharma, Hitendra Garg, Priti Dimri, "An Efficient (n, n) Visual Secret Image Sharing using Random Grids with XOR Recovery", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.11, pp.14-20, 2019. DOI: 10.5815/ijcnis.2019.11.02