International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Collusion Attacks in XOR Based RG-VSS

Mainejar Yadav, Ranvijay

Abstract: ***Visual secret sharing (VSS) is a well-known technique from the past few decades for data security. Recently, XOR based VSS has attracted many researchers due to its lossless or good visual quality of reconstructed secret image. Cheating in visual cryptography based VSS was introduced by Horng et. al. in 2006. Cheating occurs when a dishonest participant presents fake share and performs stacking of fake share with honest participants who have genuine share, thereby revealing the fake secret image instead of the original secret image. Cheating occurs when some XOR based VSS are exposed to collusion attacks. Here, in this paper, we have demonstrated and proved that there is a security issue in existing XOR based VSS schemes.***

Index Terms**: *Cheating problem, Collusion attack, Random grids, Visual secret sharing.***

I. INTRODUCTION

Secret sharing was first introduced by A. Shamir (1979) [1] and G. Blakley (1979) [6]. According to this technique, secret information is divided into n number of pieces, and is recovered by using k number of pieces out of n. Visual secret sharing (VSS) is a variant of secret sharing where the information remains in the form of an image. In (k, n) VSS, the secret image is divided into n number of parts or shares, and at the time of reconstruction at least k out of n number of shares are required. There are many applications of VSS like information hiding (W.P. Fang & J.C. Lin, 2006), visual authentication and identification [9], access control, image encryption [3], [12] and water marking [14] etc. Visual Cryptography (VC) [8] is one of the various types of existing VSS techniques, in which encoding and decoding is done by the codebook. For instance, codebook used in (2,3) VC is shown in Table I. In this codebook SH_1, SH_2 and SH_3 show the generated shares. Whenever any two out of three shares are stacked together, the secret image can be recovered.

Security issue is a big concern in visual cryptography based VSS. At the time of reconstruction of secret, one participant (dishonest) known as cheater, may release a fake share. In this case, only cheater has the opportunity to recover the original secret, while the other shareholders (honest participants) will get the fake secret. The cheating problem in VC based VSS was introduced by Horng et al. (2006) [7].

Suppose, there are three participants P, Q and R, where P, Q are dishonest participants, and R is an honest participant. P and Q want to cheat R by changing some black pixels into white pixels (shown in Row 1 of Table II) and changing some white pixels into black pixels (shown in Row 3 of Table 2).

Another type of VSS based on Random Grids (RG-VSS) was introduced by O. Kafri and E. Keren (1987) [10]. In this type of VSS, the generated shares are called random grids that have the same size as that of secret image and the process of reconstruction of secret image is same as in VC. RG-VSS has the following advantages over VC: (1) generated share size is same as the size of secret image i.e. the pixel expansion is 1 and (2) codebook is not required. S.J. Shyu (2007) [13] introduced the (2, 2) RG-VSS for grayscale and color images. A more generalized version of (S.J. Shyu, 2007) was proposed by T.H. Chen and K.H. Tsao (2009) [15] as (2, n) and (n, n) RG-VSS. (k, n) threshold based RG-VSS was given by T.H. Chen and K.H. Tsao (2011) [16]. The cheating problem also exists in RG based VSS, as suggested by Y. S. Lee and T.-H. Chen (2012). Many researchers have worked on cheating attacks and cheating prevention techniques (G.B. Horng et al., 2006 [7]; R.D. Prisco & A.D. Santis, 2006 [11]; D.S. Tsai et al., 2007 [5]; C.M. Hu & W.G. Tzeng, 2007 [2]). The poor visual quality of reconstructed secret image is a vital challenge in OR based VC and VSS. XOR based RG-VSS (RG-XVSS) is a new technique which improves the visual quality of reconstructed secret image. D. Ou et. al. (2015) [4] proposed a RG-XVSS, where the generated shares are meaningful. Many researchers have worked on RG-XVSS, but here our focus is on a technique proposed by X. Yan et al. (2015) [17]. In this paper, we have analyzed the RG-XVSS and the experimental results show that collusion attack is possible in such types of schemes.

The remaining part of the paper is organized as follows. In Section 2, we discuss the possibility of collusion attack in (k, n) RG-XVSS and test the feasibility of cheating in that scheme. Section 3 shows the experimental results. Conclusion and future work are given in Section 4.

II. COLLUSION ATTACK IN (K,N) RG-XVSS

This section demonstrates that the collusion attack may work in (k, n) RG-XVSS (X. Yan et al., 2015 [17]).

A. Collision Attack Scenario in (k, n) RG-XVSS

The collusion attack or cheating process in (k, n) RG-XVSS is shown in Figure 1. Here, secret image is encoded into n number of shares/random grids(RG) and these shares (RG_1, RG_2, RG_3, RG_4,….) are distributed among Alice, Bob, Carol, Sam and other participants. Assume that, Alice, Bob and Carol are dishonest participants and Sam is an honest participant. Alice, Bob and Carol reconstruct the secret image by using their shares and recover the lossless secret image by using the reconstructed image. Dishonest participants choose the cheating message/ fake secret (FS).

Manuscript published on 30 August 2019.
***Correspondence Author(s)**
Mainejar Yadav, CSED, MNNIT ALLAHABAD, Prayagraj, India.
Ranvijay, CSED, MNNIT ALLAHABAD, Prayagraj, India.

Table I. Codebook used in (2,3) Visual Cryptography

Secret Image	SH_1	SH_2	SH_3	$SH_1 \oplus SH_2$	$SH_1 \oplus SH_3$	$SH_2 \oplus SH_3$
□						
■						

Table II. Example of cheating process in (2,3) Visual Cryptography.

Secret Image	Fake Image	SH_1	SH_2	SH_3	SH_1	SH_2
■	□					
■	■					
□	■					
□	□					

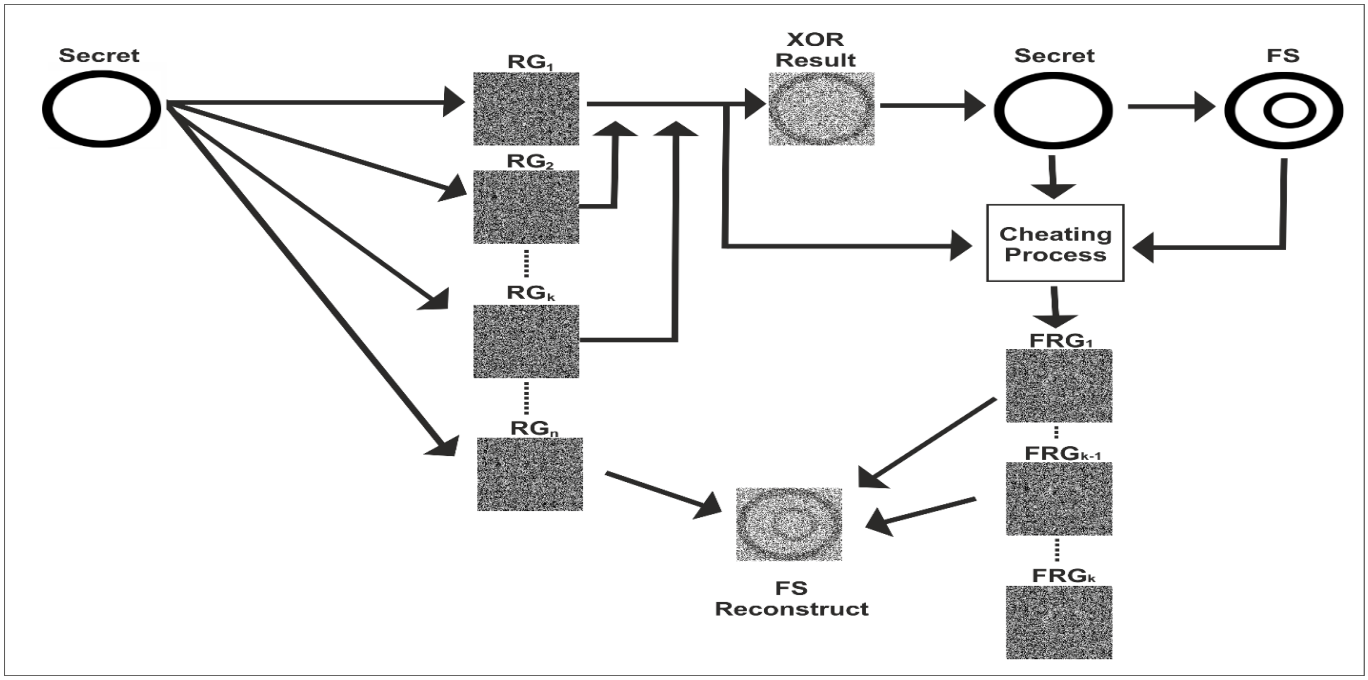

Fig. 1. Example of cheating process in (k, n) RG-XVSS.

Retrieval Number: J87830881019/19©BEIESP
DOI: 10.35940/ijitee.J8783.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

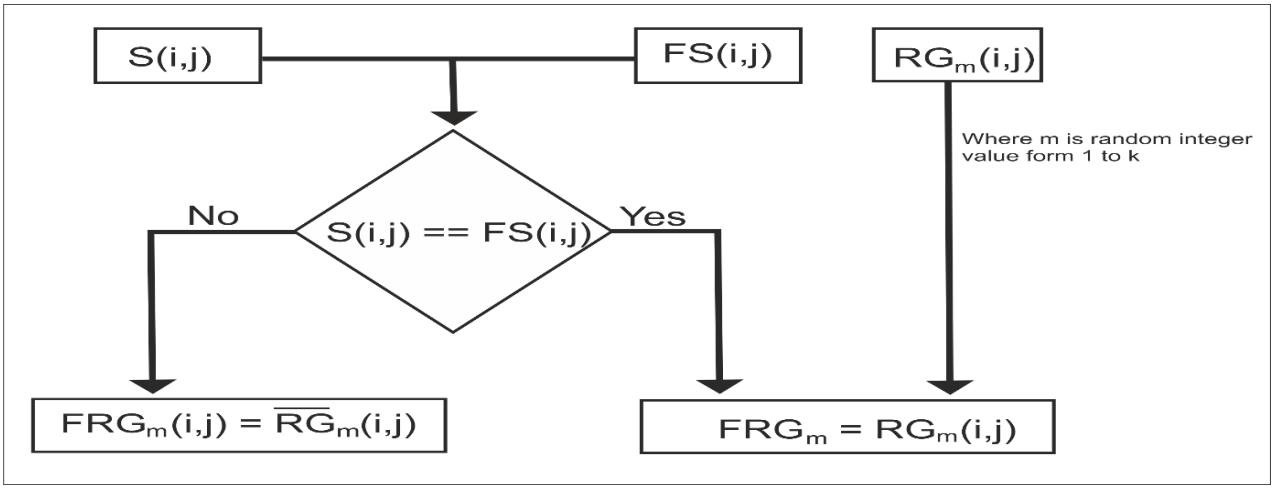

Fig. 2. Fake random grids generation process in (k, n) RG-XVSS

Cheating message is created by changing some white pixels into black pixels in the original secret image. After that collusion attack is performed to generate fake random grids (FRG). When Sam performs X-OR operation on his random grid (RG_n) and other fake random grids (FRG_1, … FRG_{k-1}), the fake secret/cheating message is revealed.

B. Review of (k, n) RG-XVSS [20]

k random grids pixels are generated by using VCS [10], [16] and remaining (n-k) random grids pixels are generated randomly. For giving equal weightage to each random grid, the generated pixels are uniformly distributed among the random grids. For reconstructing the lossless secret image, if the result of X-OR on all the grids is not equal to the pixel value of secret image then choose randomly any grid pixel from $(k+1)^{th}$ grid to n^{th} grid and complement this randomly chosen grid pixel. At the time of reconstruction of secret image, ORing/X-ORing is done of any k out of n random grids. The quality of reconstructed secret image obtained by using XOR is better than in case of using OR operation. For lossless reconstruction, the participation of all the random grids is essential.

C. Collusion Attack method in (k, n) RG-XVSS

This section presents our proposed method for collusion attack. The proposed Fake random grids generation process in (k, n) Visual Secret Sharing is shown in Figure 2 and collusion attack process is illustrated by *Collusion attack on RG-XVSS* algorithm 1.

Algorithm 1: Algorithm for Fake random grids generation in RG-XVSS

Input: k random grids RG_1, RG_2…..RG_k and a fake secret image FS, each have R x C pixels.

Output: k fake random grids FRG_1, FRG_2…..FRG_k, each have R x C pixels.

***Step* 1:** Reconstruction of secret image

$$RG_1 \oplus RG_2 \oplus - - - - - - - - - - - - \oplus RG_k = S_1$$

// S_1 *is reconstructed secret image*

Step 2: From reconstructed secret image S_1 to recovered original secret image S lossless

Step 3: Fake random grids generation,

Select randomly RG from 1 to k and generates FRG_1 to FRG_k

If ((S(i,j) == FS(i,j))

$$FRG_m(i,j) = RG_m(i,j)$$

// m is an integer value from 1 to k

else

$$FRG_m(i,j) = \neg RG_m(i,j)$$

Step 4: Repeat step 3 until all the pixels of secret image are processed

In the first step, cheaters reconstruct the secret image by using their random grids, and in the second step they use the reconstructed secret image to recover the original (lossless) secret image. Suppose, random grids RG_1 to RG_k are dishonest participant grids. In the third step, fake grid pixels are generated (as shown in figure 4). Here, any one random grid out of k random grids/shares is randomly selected and fake random grids are generated. The process of generating pixels corresponding to each grid is based on the following rule - If the pixels of secret and fake secret are same, then fake random grid FRG_m pixels are same as the pixel of RG_m, otherwise complement of the pixel of RG_m is taken. The third step is repeated for R x C number of times, where R x C is the total number of pixels present in the original secret image.

Cheating process in RG-XVSS:

After the fake random grids generation, if any (k-1) fake random grids are XORed with any random grid, the fake secret image gets revealed i.e. $FRG_1 \oplus FRG_2 \oplus FRG_3 \oplus \ldots\ldots \oplus FRG_{k-1} \oplus RG_i = FS$ (*where i is an integer value from (k+1) to n)* and when all the random grids (k fake random grids and (n-k) random grids) are XORed with each other, the reconstructed fake secret is lossless, which is shown through experimental results. The reconstruction of fake secret image can be done in two ways-

(1) By using OR operator - in this case the quality of reconstructed fake secret image is not good as compared to the result of XOR operation and it only works on (n, n) RG-XVSS.

(2) By using XOR operator - reconstruction of fake secret image will be done for both the cases (k, n) as well as (n, n) with good visual quality as compared to that obtained from OR operation.

D. Feasibility of Cheating in (k, n) RG-XVSS

The feasibility of collusion attack is checked by the following two steps:

1. The generated fake shares are random grid or not.
2. The reconstructed fake secret image will be visible or not.

Proposition 1: Fake shares are meaningless: The generated fake shares should be noise like random grid because victims do not get extra attention on the fake shares.

Proof: In proposed (k, n) RG-XVSS cheating process, k (FRG_1 to FRG_k) number of fake shares are generated. These shares are either same as RG_1 - - - - - - - RG_n or complement of RG_1 - - - - - RG_n of fake shares FGR_1 - - - - - -FGR_k respectively. Suppose, light transmission of white & black pixels in fake shares are L[FRG(FM_0)] and L[FRG(FM_1)] respectively. In Ref. (T.H. Chen & K.H. Tsao, 2009), the grid pixels are generated in RG_1 for black & white pixels with probability of 1/2. Hence, the expected light transmission of L[FRG (FM_0)] = L[FRG(FM_1)] = 1/2 . So, according to the definition of contrast, the false random grids are meaningless.

Lemma 1: If all the shares are XORed with each other, the reconstruction of fake secret will be lossless.

Proof: Suppose a secret image S is divided into n number of random grids RG_1, RG_2, - - - - - - - RG_n. In Ref. (X. Yan et al., 2015), when all grids are XORed with each other, the recovered secret image is lossless and at least k (1<k>=n) number of shares are required to reconstruct the secret image. Suppose, fake secret image is FS.i.e.,

$$RG_1 \oplus RG_2 \oplus \dots \oplus RG_n = S \quad (1)$$

suppose,

$$RG_{k+1} \oplus \dots \oplus RG_n = VRG \quad (2)$$

And when only k grids are XORed with each other, lossy secret image S_1 will be recovered. i.e.,

$$RG_1 \oplus RG_2 \oplus \dots \oplus RG_k = S_1 \quad (3)$$

Suppose, cheaters have RG_1 to RG_k random grids, so they will recover the secret image S_1 and by using S_1 the original secret image S will be recovered.

from equation (1) and (2)

$$RG_1 \oplus RG_2 \dots \oplus RG_k \oplus S = RG_{k+1} \oplus \dots \oplus RG_n = VRG \quad (4)$$

So, cheater has RG_1 to RG_n grid along with original secret S. So, from equations 2 and 4, we can say, they will set the victim random grid VRG pixel's value and cheater generates the fake random grid FRG in the following way-

$$FRG_1 \oplus FRG_2 \oplus \dots \oplus FRG_k = FRG \quad (5)$$

Since FRG(i,j)= FS(i,j) $\oplus$ VRG(i,j) so,

$$FRG(i,j) \oplus VRG(i,j) = FS(i,j) \quad (6)$$

During decoding process, the secret image

$$FRG_1 \oplus \dots \oplus RG_{k+1} \oplus \dots \oplus RG_n = \text{Recovered image} \quad (7)$$

From equations 2, 5 & 7

$$FRG \oplus VRG = \text{Recovered image} \quad (8)$$

From equations 6 and 8

Recovered image = FS

So, we can say that recovered image is lossless fake secret image.

III. Experimental Results

Simulation: Figure 3 shows the experimental results of (k, n) RG-XVSS (X. Yan et al., 2015), where k=3 and n=4. A binary secret image S of size 512 x 512 is shown in Fig 3 (a), the generated random grids RG_1, RG_2, RG_3 and RG_4 are shown in Fig 3 (b)-(e), Fig 3 (f)-(i) shows the XORing result of any three random grids. Figure 3 (j) shows the XORing of all four random grids. To test the feasibility of cheating by collusion attacks in (k, n) RG-XVSS (X. Yan et al., 2015), where k=3 and n=4, simulation is conducted and results are shown in Fig 4. A binary fake/cheating secret image FS is shown in Fig 4 (a), the generated fake random grids FRG_1, FRG_2, and FRG_3 are shown in Fig 4 (b)-(d), Fig 4 (e)-(g) show the XORing result of any two fake random grids with random grid RG_4. Figure 4(h) shows the XORing of all three fake random grids with random grid RG_4. These experimental results clearly show that cheating is possible by collusion attacks in (k, n) RG-XVSS [17].

IV. Conclusion

RG-XVSS is a very popular technique due to its good visual quality of reconstructed secret image. It also provides lossless reconstruction. In VSS, cheating due to collusion attack is a major security issue. The experimental and theoretical analysis have proved that the proposed collusion attack is possible in (k, n) RG-XVSS (X. Yan et al., 2015). The techniques for preventing collusion attack will be taken as future work consideration.

Retrieval Number: J87830881019/19©BEIESP
DOI: 10.35940/ijitee.J8783.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

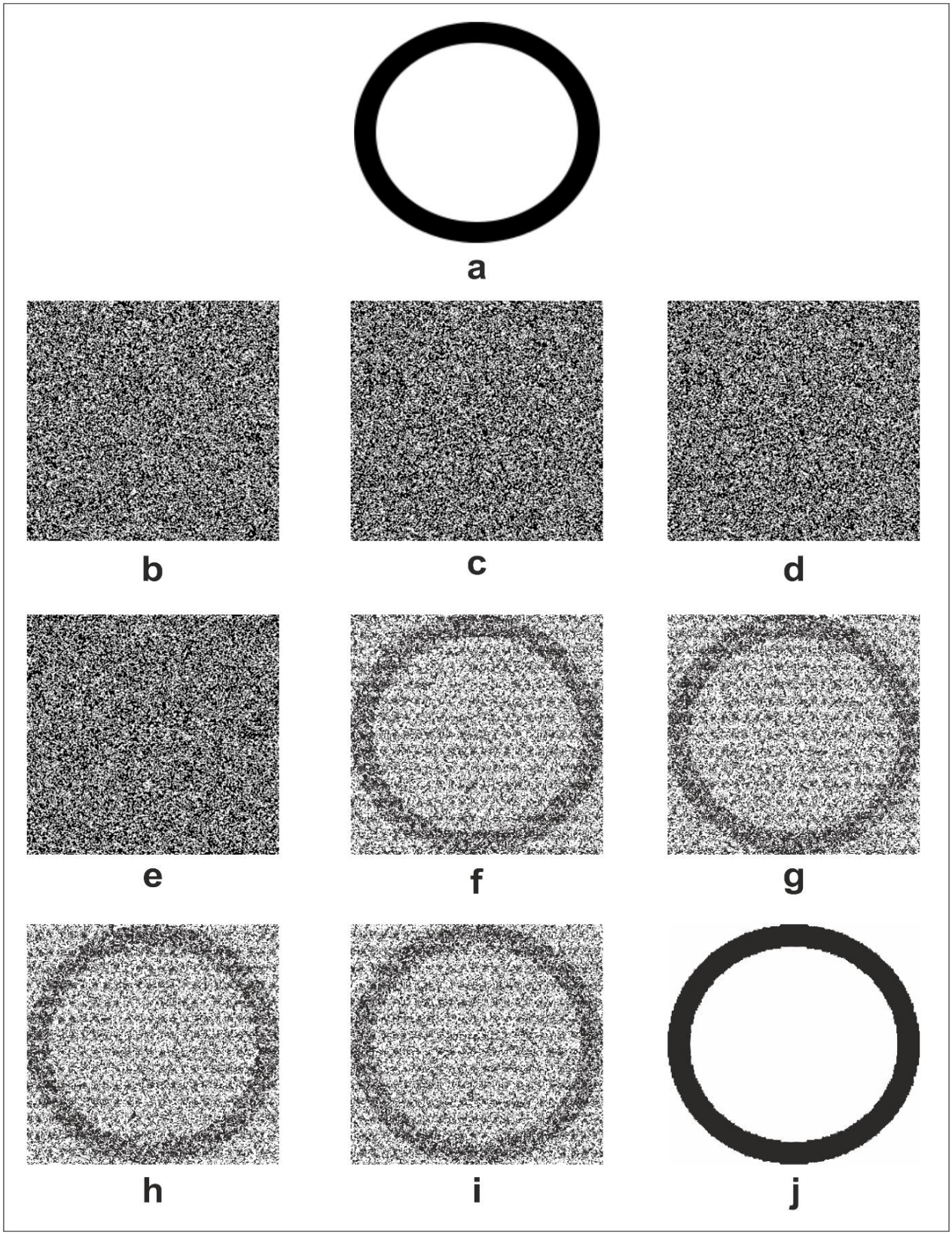

Fig. 3. a. Original secret image, b. RG_1, c. RG_2 d. RG_3, e. RG_4, f. $RG_1 \oplus RG_2 \oplus RG_4$, g. $RG_1 \oplus RG_3 \oplus RG_4$, h. $RG_1 \oplus RG_2 \oplus RG_3$, i. $RG_2 \oplus RG_3 \oplus RG_4$, j $RG_1 \oplus RG_2 \oplus RG_3 \oplus RG_4$.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

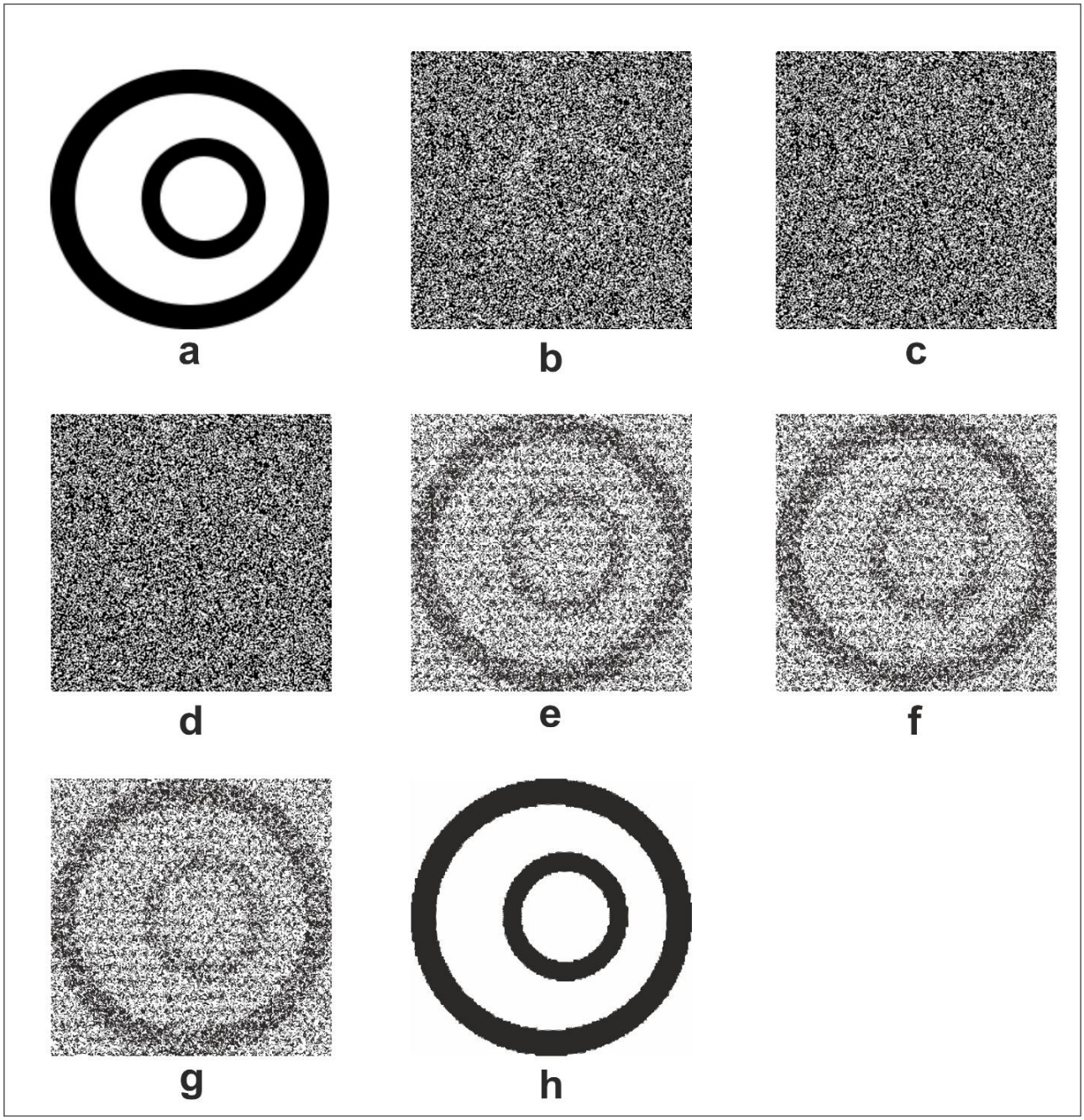

Fig. 4. a. FS, b. FRG_1, c. FRG_2 d. FRG_3, e. $FRG_1 \oplus FRG_2 \oplus RG_4$, f. $FRG_1 \oplus FRG_3 \oplus RG_4$, g. $FRG_2 \oplus FRG_3 \oplus RG_4$, h. $FRG_1 \oplus FRG_2 \oplus FRG_3 \oplus RG_4$

REFERENCES

1. A.Shamir (1979) "How to share a secret", *Communications of the ACM*, 22, 612–613.
2. C.M. Hu, W.G.Tzeng (2007) "Cheating prevention in visual cryptography", *IEEE Transactions on Image Processing*. 16(1), 36–45.
3. C.N. Yang, A.G.Peng, T.S.Chen (2009) "MTVSS: Misalignment Tolerant Visual Secret Sharing on resolving alignment difficulty", *Signal Processing*. 89(8), 1602–1624.
4. D. Ou, W. Sun and X. Wu. (2015) "Non-expansible XOR based visual cryptography scheme with meaningful shares", *Signal Processing*. 108,604-621.
5. D.S.Tsai, T.H.Chen, G.Horng (2007) "A cheating prevention scheme for binary visual cryptography with homogeneous secret images", *Pattern Recognition*, 40(8), 2356–2366.
6. G.Blakley (1979) "Safe guarding cryptographic keys", *AFIPS Conference*. 313–317.
7. G.B.Horng, T.H.Chen, D.S.Tsai (2006) "Cheating in visual cryptography", *Designs, Codes and Cryptography*. 38(2), 219–236.
8. M.Naor, A. Shamir (1994) "Visual cryptography", *Advance in Cryptology: Eurocrypt94, Lecture Notes in Computer Science*. 950, 1–12.
9. M.Naor, B.Pinkas (1997) "Visual authentication and identification. *International Cryptology Conference on Advances in Cryptology", Lecture Notes in Computer Science.* 1294, 322–336.
10. O.Kafri, E.Keren (1987) "Encryption of pictures and shapes by random grids", *Optics Letters*. 12(6), 377–379.
11. R.D.Prisco, A.D.Santis (2006) "Cheating immine (2,n)-threshold visual secret sharing scheme. *Security and Cryptography for Networks", Lecture Notes in Computer Science*. 4116.
12. R.Lukac, K.N. Plataniotis (2005) "Bit-level based secret sharing for image encryption", *Pattern Recognition.* 38(5), 767–772.

Retrieval Number: J87830881019/19©BEIESP
DOI: 10.35940/ijitee.J8783.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

13. S.J.Shyu (2007) "Image encryption by random grids", *Pattern Recognition.* 40, 1014–1031.
14. T.H.Chen, D.S.Tsai (2006) "Owner–customer right protection mechanism using a watermarking scheme and a watermarking protocol", *Pattern Recognition*. 39(8), 1530–1541.
15. T.H.Chen, K.H.Tsao (2009) "Visual secret sharing by random grids revisited", *Pattern Recognition*. 42, 2203–2217.
16. T.H.Chen, K.H.Tsao (2011) "Threshold visual secret sharing by random grids" *Journal of Systems and Software*. 84, 1197–1208.
17. X.Yan, S. Wang, X. Niu and Ching-Nung Yang (2015) "Random grid based visual secret sharing with multiple decryptions", *J. Vis. Commun. Image R.* 26, 94-104.
18. Yao-Sheng Lee, Tzung-Her Chen (2012) "Insight into collusion attacks in random-grid-based visual secret sharing", *Signal Processing.* 92,727-736.

AUTHORS PROFILE

Mainejar Yadav received B.Tech degree from UPTU Lucknow, M.Tech degree from MNNIT, Allahabad and presently pursuing Ph.D. in CSE from MNNIT Allahabad. He is Assistant Professor of Computer Science and Engineering Department in RAJKIYA ENGINEERING COLLEGE Sonbhadra, Utter Pradesh. His areas of interests include Visual Cryptography, Digital Watermarking and Network Security.

Ranvijay received M.Tech and Ph.D. Degree from MNNIT Allahabad. He is Assistant Professor of Computer Science and Engineering Department in MNNIT Allahabad, Prayagraj, Utter Pradesh. His contributions in various international and national Journals. His area of interests includes Visual Cryptography, Network Security and Real time system.