Secret Sharing Schemes using Thresholding

Abhishek Mishra
Dept. of Computer Science & Engineering
IFTM University, Moradabad (U.P.), INDIA
abhimishra2@gmail.com

Ashutosh Gupta
Dept. of CS & IT
MJP Rohilkhand University, Bareilly (U.P.) INDIA
ashutosh3333@gmail.com

***Abstract*- The secret sharing (SS) scheme can be considered as a basis for secure key management. In some practical cases, it is possible that key may be lost or damaged due to some reasons thus causing the revealing of secret more difficult. Secret Sharing is a method to hide secret information by partitioning it into multiple parts, also called shares. Each share is distributed to participants in such a way that less than k participant among n participant has no knowledge about the secret but k or more than k participant can recover the secret. This paper proposes two schemes namely, probabilistic (2, 2) SS scheme and (2,2) visual secret sharing (VSS) scheme using threshold and Boolean operation. These schemes generate random matrices and some threshold parameter to generate shares of secret image. The experimental results show that the proposed scheme is significantly less prone to security attacks, reasonable computation overhead in terms of time and minimum pixel expansion.**

Keywords- cryptography, secret sharing, shadow image, boolean operation.

I. Introduction

Defense and military area is a prime sector where sharing the secret in the past as well as in the modern days has utmost importance. Secret sharing is a active research area in the recent past. It also has its applicability in digital media where security has been a subject of seriousness. These factors lead to the development of encryption and cryptography. Now days, the computer technology is in its advance stage and decryption of secret data is computationally infeasible in many respect. The security of data arises by combining the cryptographic functions and security processing methods. The secret sharing schemes involves distribution of shares in the form of information through common communication channel in such a way that no information is leaked itself by the secret data since information is sent to users in multiple parts. When these multiple parts or secret shares are combined in some predefined manner, than only secret information is revealed. The shares are combined manually or it requires some electronic processing and finally secret information is recovered.

A. Secret Sharing:

The concept of secret Sharing plays an important tool in cryptography and security techniques. The secret sharing scheme can be considered as a basis for secure key management. In some practical cases, it is possible that key may be lost or damaged due to some reasons thus causing the revealing of secret more difficult. Secret Sharing is a method to hide secret information by partitioning it into multiple parts, also called shares. Each share is distributed to participants in such a way that less than k participant among n participant has no knowledge about the secret. On the other side k or more than k participant can recover the secret easily. This aspect of secret sharing has claimed to be a right tool in secure key management and multi-party secure protocols.

Secret sharing (SS) schemes was first introduced by Blakley [1] and Shamir [2] independently and known as (k, n) threshold schemes. Naor and Shamir in [3] propose the concept which allows the decoding of secret information (or images) with the help of Lagrange’s interpolation. They proposes a k out of n secret sharing scheme (SS) where k or more shares among n shares will reveal the secret but no information is leaked if less than k shares are combined [4], [5]. The n shares are computed first, than distributed to n participants. During decoding, the secret image is revealed by Lagrange’s interpolation using k or more shares. The shamir’s scheme requires a lot of expensive computation work during distribution and reconstruction phase. Example 1 shows the concept of (2,2) secret sharing.

Example 1: A straight line is a combination of many tiny points O, A, B, C, D,...., E. The coordinates of these points are distributed to n participants. The slope of line is obtained by using only two points. So minimum two points are required to obtain slope of line, this is similar to the case of (t, n) secret sharing where t = 2. The slope of line cannot be calculated if there are less than t. So, minimum two participants are required to find the secret information. This scenario is shown in Figure 1. Banking system also uses the concept of secret sharing for maintaining security of a locker. To open the locker both keys are required. (t, n) secret sharing concept applies in this case, where t = 2, n = 2.

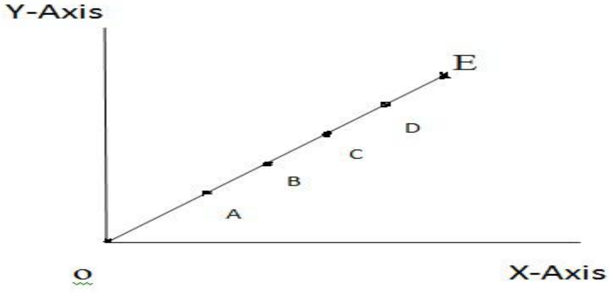


Fig.1. Illustration of (t, n) secret sharing scheme for straight line where t=2

Secret sharing concept can be applied in the field of computer security in an easy manner. Data can be encrypted using secret sharing and distributed to n participants. The original data will be decrypted be by combining predefined set of participants.

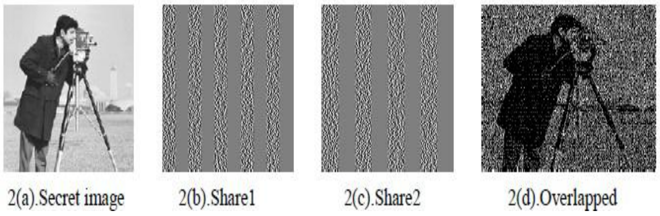
Since huge amount of data is available in image form, image encryption / decryption is an area of interest to researchers. Image data is bulky in nature so techniques like DES,AES take a lot of computation time. Providing security of image data is also the major issue. VC is a technique that is used for only image encryption /decryption. It takes less time in comparison to other existing techniques. Decryption is very much easy in visual cryptography (VC). VC does not require as much mathematical knowledge for encryption / decryption as compared to usual algorithms.

B. Visual Secret Sharing:

The concept of Visual Secret Sharing (VSS) was proposed by Naor and A Shamir[4]. VSS is based on the secret sharing in which secret image is encoded into a number of pieces called shares. At the time of decryption, take printout onto transparencies of these shares. Transparencies are stacked together physically, our human visual system (human Eye) used to obtain secret image. VSS does not require any device for decryption. So knowledge of cryptographic principle does not required at the time of decryption. This is the advantageous feature of VC over popular cryptographic scheme.

Visual Cryptographic Schemes (VCS) can be classified in four variety (2, 2), (2, n), (k, n) and (n, n) on the basis of access structure. In (2, 2) VCS, two shares are generated and distributed to the two participants. First number of pair defines the minimum number of participant required to construct secret image and second number refers to total number of shares generated in encryption process.

The 2 out of 2 scheme or (2, 2) scheme is illustrated with an example shown in Figure 2. The secret binary image “I” which is to be encoded is shown in part (a). Using the above encoding rule shown in Figure 3, each pixel p is divided into two sub pixels in each of the two shares generated, shown in Figure 2 (b-c). The result of superimposition is shown in Figure 2 (d) when the two shares are superimposed on one another resulting in an output secret image. The decoded or superimposed image is identified with meaningful information but some contrast is lost. Since, original pixel p is divided into two subpixels, the resulting size of image is twice that of original image



2(a).Secret image 2(b).Share1 2(c).Share2 2(d).Overlapped

Fig.2. Example of 2-out-of-2 scheme

The visual Secret sharing schemes generally consist of four tuples: (m, α,H(V), γ) where,

m- The number of Subpixels in a share.

α-is the relative difference in the weight between the combined shares that come from white pixel and a black pixel in the original image.

H(V) - Hamming Weight. Number of 1 in OR vector V.

γ -is the size of the collection of matrices C0 and C1. C0 refers to the sub-pixel patterns in the shares for a white pixel and C1 refers to the sub-pixel patterns in the shares for a black pixel.

C0 - all the matrices obtained by permuting the columns of S0.

C1 - all the matrices obtained by permuting the columns of S1.

Due to this pixel expansion, one pixel from the original image gets expanded into two pixels. The shares can be generated in the following manner.

1) If the pixel of the original binary image is white, randomly pick the same pattern of four pixels for both shares.

2) If the pixel of the original image is black, pick complementary pair of patterns.

C. Naor and Shamir’s scheme for encoding a binary pixel into two shares :

In the encryption process of (2, 2) Naor scheme [4] for VC, a secret image is processed in left to right and top to bottom manner. Whenever, pixel is white then column 2 of Figure 3 is chosen to generate share 1(S_1) and Share 2 (S_2). On the other hand if processed pixel is black then column 3 of Figure 3 is chosen to generate S_1 and S_2. Two Random shares S_1 and S_2 two are created. Now, each share (S_1, S_2) has two white and two black pixels corresponding to pixel P of input image. Each single share gives no clue about the pixel p whether, it is white or black. Secret image is revealed only when both shares $S_1$and S_2 are superimposed.

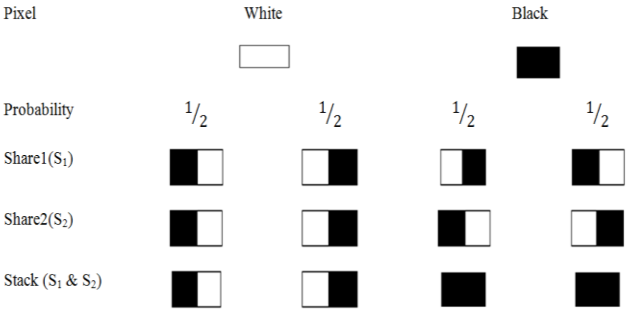


Fig.3. (2, 2) visual cryptographic scheme with m=2

II. RELATED WORK:

Various parameter considered by researchers to evaluate the performance of VSS. These are follows: (1) Contrast : Contrast loss between Secret and Reconstructed image (2)Pixel expansion : Number of pixels in share in respect of one pixel of source image (3)Alignment of shares for reconstructing secret image (4) Access Structure: set of participants to recover Secret (5)Share held by each participant: one or set of shares distributed to participant(6) Random shares or meaningful shares: share with cover image or not(7) Aspect ratio: Block of sub pixel in share with the same ratio in secret image. m should be square (8) Single secret or multi secret:

How many Secret images are encrypted at a time (9) Share management: less number of shares or meaningful shares are easily manageable (10) Idealness of scheme: Size of source image and shares.(11)Number of runs of algorithm to reconstructing secret image (12)Complexity: Number of operations in Encryption and decryption.

Over the past decade, most VSS schemes [6], [8], [9], [19], [21] for images have been implemented by simply stacking the collected shadows. The pixel expansion and low accuracy are weaknesses of these schemes as each original pixel is encoded (or expanded) into m subpixels per share (or shadow image). The (2, 2) VSS is a special case of (k, n) VSS scheme [8] and has many useful applications as discussed in section I.

Wang et al. [12] proposed two different VSS schemes based on Boolean operations. One is probabilistic (2,n) scheme, which reconstructs smaller areas significantly with good contrast. The other is deterministic (n,n) scheme, which reconstructs the secret image perfectly. In their probabilistic (2,n) scheme, the secret image is encrypted by using a set of n matrices generated randomly in such a way that the black original pixels are reconstructed perfectly, whereas the white original pixels are reconstructed correctly with probability equal to 0.5.

Ulatus et al.[7] proposed a method to construct this set of n matrices and enhanced the probability of correct reconstruction of the white original pixels to $\frac{n}{2n-2}$.

The Boolean operation-based (k, n)-threshold VSS scheme was considered by Chao and Lin [13] in 2009. In their method [13], a (k,n,m) shadow-assignment matrix is constructed having k-1 zeros and (n-k+1) ones for a suitable chosen parameter m= $\binom{n}{k-1}$ With (k,n,m) shadow-assignment matrix, m temporary shares generated by Wang et al.'s deterministic (m,m) scheme [12] are assigned to n participants. Chao and Lin's scheme [13] has the pixel expansion equal to 2 × $\frac{n-k+1}{n}$ and does not guarantee for no pixel expansion as Boolean operation-based other do.

Chen and Wu [20] in 2011 extend the Wang's deterministic (n,n) scheme [12] to a (n+1, n+1) multi secret sharing scheme, where n secret images are subsequently encoded into (n +1) meaningless share images.

Chen and Tsao [11] proposed the random grid-based (k, n)-threshold scheme with no pixel expansion and no codebook requirement. T. Guo [15] proposed a method to improve the contrast in 2013.

In 2014 Sachin Kumar and Rajendra K. Sharma [10] proposed a method of visual secret sharing which is based on Boolean operations. This scheme uses no pixel expansion, no codebook requirement, no need to align properly in decryption and can encrypt binary images as well as gray-level or colour images.

In this article, we propose a (2, 2) probabilistic secret sharing scheme using threshold in Section III-A. Section III-B describes the Proposed (2, 2) Probabilistic VSS Scheme for binary, grayscale and colour images. The experimental results and discussion is given in section IV. Finally, conclusion of work is presented in section V.

III. PROPOSED (2, 2) PROBABILISTIC SCHEME USING THRESHOLD

A. PROPOSED (2, 2) PROBABILISTIC SS SCHEME USING THRESHOLD

In this section, we propose a probabilistic (2, 2) secret sharing scheme for any kind of images including binary, gray level as well as colour images. The scheme uses a simple XOR operation to generate share images as well as to reveal the secret image. A grayscale image has gray levels from 0 to 255. Mostly the information content part of any image is closer to its maximum gray level value. For example: black pixel in the binary image has more information than white pixel. Likewise, in gray scale images, it is above some threshold grayscale value. To motivate this fact, we design the algorithm by considering some threshold for gray level. It is experimentally observed that, by setting threshold value T = 128, the information contained in the shares are completely unrecognizable as well as secret image with higher contrast is revealed after reconstruction. For our experiment purpose, we set the threshold T = 128.

The working of algorithm is as follows: First, a random share I_1 of gray scale values between (0, 255) is generated. The original secret image is read pixel by pixel and if the value of pixel is lies between 0 to threshold T, than pixel value of I_1 is copied to second share I_2, otherwise XORing between I and I_1 is copied to share I_2. In this way, pixel values 0 to T of I is simply discarded and some random values of I_1 are copied. The possibility of copying these random pixel values of I_1 may be in between 0 to 255. In the revealing phase, an explicit XOR operation is required to reveal the secret. The XOR operation between I_2 and I_1 sets all those pixels with value ”0” which are copied from I_1 to I_2 during encoding phase. Thus those pixels are visualized as black pixels; however in original image they have some other gray values. Since, we are using XOR operation to reveal the secret, this scheme is not actually a visual secret sharing as it does not require stacking the shares. To reveal the secret, XORing between shares I_1 and I_2 is required. The algorithm for proposed (2, 2) SS scheme is shown below.

```
Algorithm 1: (2, 2) Probabilistic SS Scheme using Threshold
// Distribution Phase
Pre-condition: A secret Image I of size M * N
Post-condition: Two Shares $I_1$ and $I_2$.
(1) Generate random matrix $I_1$
(2) Populate share $I_2$ according to the following rule.
        for i = 1 to M
        for j = 1 to N
            if $0 \leq I(i , j) \leq 128$
                $I_2(i, j) = I_1(i, j)$
       else
         $I_2(i; j) = I_1(i, j) \oplus I(i, j)$
      endif
         end for
         end for
```

```
  // Revealing Phase
Secret Image R = $I_1 \oplus I_2$
```

B. *Proposed (2, 2) Probabilistic VSS Scheme for binary, grayscale and color images:*

In this section, we propose a Probabilistic (2, 2) visual secret sharing (VSS) scheme using threshold, in which a secret can be revealed by directly stacking the two shares. Since the stacking operation is similar to the ORing operation so this scheme can be considered as a slight modification in revealing phase and considered under the category of VSS. It is experimentally observed that if use OR operation instead of using XOR operation, than scheme behaves like a visual secret sharing (VSS). This slight change converts the SS scheme into a probabilistic based VSS scheme. This observations leads to a conclusion that scheme has a nice property that secret image is revealed either by XORing or ORing of two shares. The ORing operation can be done manually but XORing require a computer software or some hardware (like copy machine) in which it is implemented. The Boolean expression $A \oplus B$ is same as $\overline{\overline{((A\overline{B}))}.\overline{((\overline{A}B))}}$ and can be implemented by five NAND gates. This hardware is added to any copier machine to reveal the secret. Next, we show the explanation of the property mentioned above.

Let original pixel of image I at position (x, y) is 67. Since its value lies in between 0 to 128, a random pixel value of secret share I_1 from position (x, y) is copied to second share I_2 at same position (x, y). Assume I_1s pixel value is 167 and its binary equivalent is: $(01000011)_2$.

Then, $I_2 = I_1 = 167 = (01000011)_2$

Next, we show the difference between revealing phase of algorithm 1 and algorithm 2. Revealing of algorithm 1 requires bitwise XOR between I_1 and I_2, which is:

$I_1 \oplus I_2 = (01000011)_2 \oplus (01000011)_2 = (00000000)_2 = 0$ (a black pixel).

In Algorithm 2, we use bitwise OR between I_1 and I_2:

$I_1 + I_2 = (01000011)_2 + (01000011)_2 = (01000011)_2 = 67$ (gray level value).

From the above, it is clear that XOR produces black pixels at those positions where original pixel values lies in between 0 to 128, while OR produces some random value of I_1 Hence the property.

Algorithm 2: (2, 2) Probabilistic VSS Scheme using Threshold:

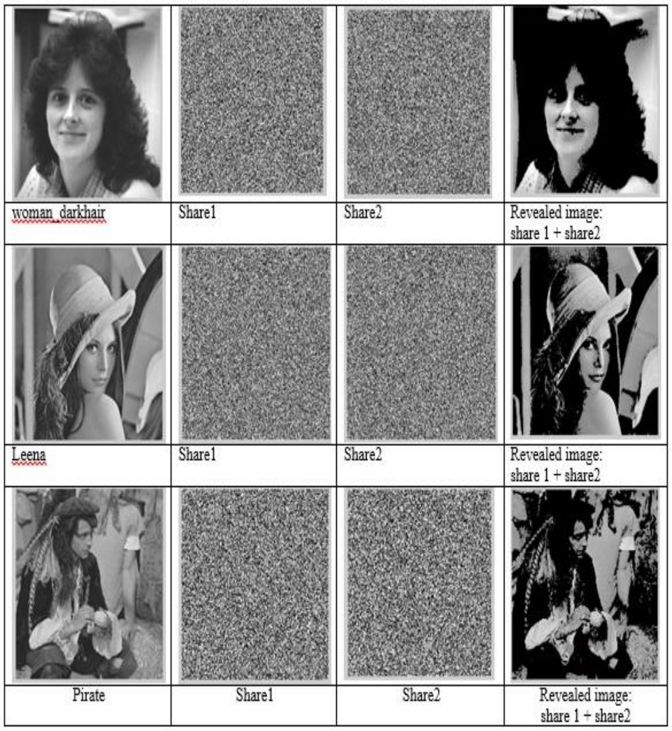
```
// Distribution Phase
Pre-condition: A secret Image I of size M * N
Post-condition: Two Shares $I_1$ and $I_2$.
 (1) Generate random matrix $I_1$ s.t. each element of $I_1$ € 0, 255.
(2) //Populate share I2 according to the following rule.
for i = 1 to M
for j = 1 to N
      if $0 \leq I(i, j) \leq 128$
         $I_2(i, j) = I_1(i, j)$
   else
         $I_2(i, j) = I_1(i, j) \oplus I(i, j)$
     endif
 end for
 end for

// Revealing Phase
          Secret Image R = $I_1 + I_2$
```

C. *Extension of (2, 2) schemes into Strict (2, n) scheme:*

The secret sharing and visual secret sharing schemes described in section III-A and III-B are well extended to strict (2, n) scheme. The notion of strict (2, n) scheme is explained below. Note that in these two schemes, we generate a random matrix as first share and assume that it is publicly known to everyone. The second share is generated with the help of first share (public share) and some secret image. By strict (2, n) scheme we mean that among 'n' shares (or users), one share is publicly known to everyone, while each (n-1) share (or user) when combined with public share will reveal its corresponding secret image. Thus, the meaning of first term in (2, n) is included in second term.

This strict (2, n) extension can be applied to many applications, like embedding the second share into the credit/debit card to identify a person. Suppose he/she pay some bill to any shopping mall and shows his/her debit card to the cash counter. The billing counter uses the public share and credit/debit card to compute the secret image (may be photograph of card holder). If the revealed image is of same person who submitted the card to the cash counter, the amount is successfully debited otherwise bill counter refuses him/her to make payment.

III. Experimental Results and Discussion:



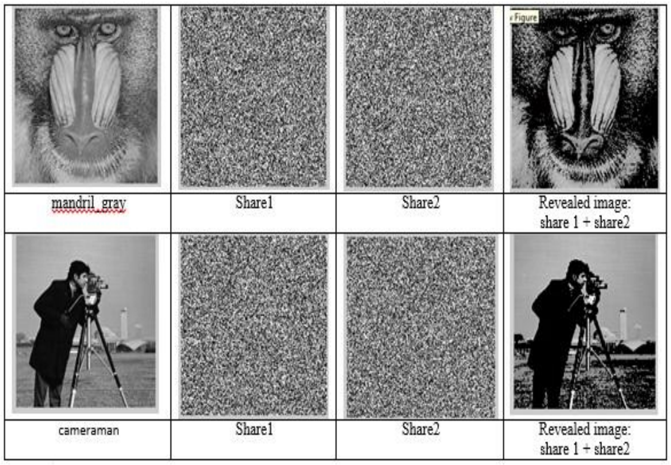

mandril_gray
Share1
Share2
Revealed image: share 1 + share2
cameraman
Share1
Share2
Revealed image: share 1 + share2

Fig.4. Secret shares with their corresponding secret images.

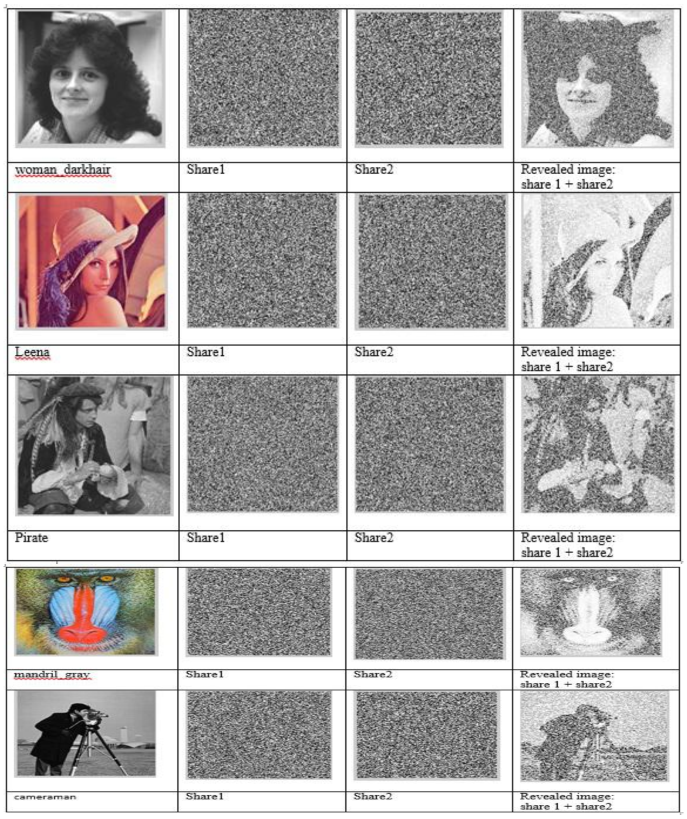

woman_darkhair
Share1
Share2
Revealed image: share 1 + share2
Leena
Share1
Share2
Revealed image: share 1 + share2
Pirate
Share1
Share2
Revealed image: share 1 + share2
mandril_gray
Share1
Share2
Revealed image: share 1 + share2
cameraman
Share1
Share2
Revealed image: share 1 + share2

Fig 5: Secret shares with their corresponding secret images

TABLE 1: Observation of PSNR on different source images

Source Image	**Image Type**	**PSNR(db) (Algorithm1)**	**PSNR(db) (Algorithm2)**
Woman	Gray scale	17.0949	14.3271
Lena	Gray scale, Colour	18.0897	10.6587
Pirate	Gray scale	22.8745	18.7090
Mondrial	Gray scale, Colour	23.4580	11.8900
Cameraman	Gray scale	18.4501	12.3260

In this section, we provide experimental results to illustrate the effectiveness of the proposed methods. The experiments are carried on various images. The results of the proposed methods are implemented in MATLAB 7.9 running on Windows 7 computer.

The proposed (2, 2) secret sharing scheme is analyzed on different images. Figure 4 and Figure 5 shows the result of applying (2, 2) SS scheme and (2,2) VSS Scheme respectively on different gray level images including woman, Leena, pirate, mandrial and cameraman each of size 512 x 512. The shares are labeled as share 1 and share 2 for respective images and their revealed images are shown next to them. Since we have set a threshold value to eliminate unimportant pixel information, the revealed image is not exactly same as original image but still it is in verifiable stage with enhancement in contrast. Usually, the pixels with lower gray level values are surrounded with similar gray level values and if smaller value is XORed with higher value than result is a higher value. Due to this reason many of the pixels are enhanced in contrast.

In this section, we provide analysis to demonstrate our results of the algorithm 1 and algorithm 2. The experimental results show that our proposed schemes have the following observations:

1) Since random matrices of same size as original image is considered, there is no pixel expansion (m = 1). The reconstruction require XORing between two shares for algorithm1 and OR operation for algorithm 2.

2) The quality of the reconstructed secret images is satisfactory as shown in Figure 4 and Figure 5. On the basis of table 1 peak signal Noise ratio(PSNR) grater than 10db which is accepted value for gray scale and colour image.

3) Probability of attack on secret image is significantly reduced. A single share is not sufficint to generte the second share,so scheme is significantly less prone to security attacks.

4) The proposed Probabilistic (2, 2) scheme is robust to any security attack because of the random nature of gray level matrix. A random gray level image (gray scale lies in between (0-255) of size 512×512 has $256^{512*512}$ possible matrices. Generating an exact matrix that is same as a matrix used for encoding is a computationally infeasible. Thus our proposed scheme is robust to any security attack.

5) The computation complexityof traditional secret sharing scheme [2] is $O(n\log^2 n)$ for computation of polynomial and Lagranges interpolation. The algorithmic complexity of Thien et al. (k, n) threshold scheme is the same as that of Shamirs. A secret image using k shadows is revealed with computation complexity proportional of k(O(k)) and proportional to the size of the shadow images. In our scheme, the computation complexity of revealing phase of Algorithm 1 in our (2, 2) scheme require XORing of two shares, which require O(k) time, where k =2 is number of shares and processing of each share is proportional to the size of the share.

6) A comparision among the existing visual secret sharing schemes and proposed scheme is given on the basis of four parameters: 1)pixel expansion 2) operation used in encryption and decryption process 3) codebook requirement 4) computation operation involved in decryption per pixel. Table 2 shows the comparision result.

TABLE 2:Comparison among the proposed schemes and existing schemes.

Schemes	**Type**	**Pixel Expansion**	**Operation**	**Codebook requirement**	**Computation involved in decryption (per pixel)**
Moni and Naor	(k,n)	Yes	Visual cryptography	Yes	No computation required
Wang et al.	(n, n)	No	Boolean	No	O(n)
Ultas et al.	(2,n)	No	Boolean	No	1- XOR operation
Chao and Lin	(k,n)	Yes	Boolean	No	3- XOR operations
Sachin and Rajendra	(k,n)	No	Boolean	No	O(k)
Proposed Scheme Algorithm1	(2,2)	No	Boolean	No	1- XOR operation
Proposed Scheme Algorithm2	(2,2)	No	Boolean/Visual cryptography	No	1- OR operation

These schemes are the combination of boolean secret sharing scheme and random grid based secret sharing scheme. In generating share S2 boolean operation is used and in generating share S1 random grid method is used. By applying this approach our proposed scheme takes less computation time in encryption and decryption, robust to any security attack because of the random nature of gray level matrix. This methodology differentiate our proposed schemes with other existing schemes. So on the basis of avobe ovservations it is clear that our proposed schemes are more secured, minimum pixel expansion and less computation time in encryption and decryption. Schemes available in literature restricted to (2, 2) access structure or used only for binary or gray scale images. Our proposed scheme can be extended to (k, n) easily on the basis of (2, n) scheme discussed in section III-C. Proposed scheme can be applied for binary, gray scale and colour image easily.

V. CONCLUSION

In this paper, two schemes are proposed: (2, 2) probabilistic secret sharing scheme and (2, 2) probabilistic visual secret sharing scheme, with threshold parameter in encryption and boolean operation XOR and OR in decryption. These schemes have the property that there is no pixel expansion occurs during the encoding phase. Due to this behaviour problem of resolution of reconstructed image not arise in these proposed algorithms. Visual quality of reconstructed source image is good, due to acceptable value of PSNR between source image and reconstructed image observed. We also compare our schemes with other existing schemes in terms of pixel expansion, operation involved in encoding and decoding, computational complexity in decoding and security. Our schemes are secure and have used a little computational cost in the reconstruction phase. The proposed schemes may be used in applications such as image encryption, visual authentication, and copyright protection.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers for their constructive suggestions.

REFERENCES

[1] G. Blakley, “Safeguarding cryptographic keys,” in Proceedings of the 1979 AFIPS National Computer Conference. Monval, NJ, USA: AFIPS Press, 1979, pp. 313–317.

[2] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[3] M. Naor and A. Shamir, “Visual cryptography.” Springer-Verlag, 1995, pp. 1–12.

[4] C. Base, M. Naor, and A. Shamir, “Visual cryptography ii: Improving the contrast via the cover base,” 1996.

[5] W.-Q. Yan, D. Jin, and M. S. Kankanhalli, “Visual cryptography for print and scan applications.” in ISCAS (5), 2004, pp. 572–575

[6] H. Krawczyk, “Secret sharing made short,” in Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO ’93. London, UK, UK: Springer-Verlag, 1994, pp. 136–146.

[7] A. G. M.Ulutas, V.V. Nabiyev, “A pvss scheme based on boolean operations with improved contrast,” in in proc 2009 int.Conf. on Network and Service Security. IEEE, 2009, pp. 1–5.

[8] S. M. Maneesh kumar, “Visual cryptography for black and white images,” nternational Journal of Information and Computation Technology, vol. 3, no. 11, pp. 1149–1154, 2013

[9] R.-J. Hwang, “A digital image copyright protection scheme based on visual cryptography,” Tamkang journal of Science and Engineering, vol. 3, no. 2, pp. 97–106, 2000.

[10] Sachin Kumar and Rajendra K. Sharma,” Threshold visual secret sharing based on Boolean operations”, SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2014; Vol7,p.p.653–664.

[11] Chen TH, Tsao KH. Threshold visual secret sharing by random grids. Journal of Systems and Software 2011; 84:1197–1208

[12] Wang D, Zhang L, Ma, Li X. Two secret sharing schemes based on Boolean operations. Pattern Recognition 2007; 40(10): 2776–2785.

[13] Chao KY, Lin JC. Secret image sharing: a Boolean operations based approach combining benefits of polynomial based and fast approaches. International Journal of Pattern Recognition and Artificial Intelligence 2009; vol. 23p.p.263–285.

[14] Wu, X., Sun, W.:” Improving the visual quality of random grid-based visual secret sharing.” Sig. Process. Vol.93, p.p.977–995 (2013)

[15] Guo, T., Liu, F., Wu, C.: “Threshold visual secret sharing by random grids with improved contrast.” J. Syst. Software.vol. 86, p.p. 2094–2109 (2013)

[16] Yan, Xuehu,Chen, Guohui,Yang, Ching-Nun, Cai, Song-Ruei” "Random Girds-Based Threshold Visual Secret Sharing with Improved Contrast by Boolean Operations" "Digital-Forensics and Watermarking: 13th International Workshop, IWDW 2014, Taipei, Taiwan, October 1-4, 2014,LNCS 9023 P.P.319-332, 2015

[17] Hiroki Koga, Etsuyo Ueda,” Basic Properties of the *(t, n)* Threshold Visual Secret Sharing Scheme with Perfect ReAlgorithm of Black Pixels” Designs, Codes and Cryptography, Springer, July 2006, Volume 40, Issue 1, pp 81-102.

[18] B. Y. Liguo Fang, “Research on pixel expansion of (2,n) visual threshold scheme,” in 1st International Symposiumon Pervasive Computing and Applications. IEEE, 856-860.

[19] V. Rishiwal and A. Gupta, “An efficient secret image sharing scheme,”World Applied Programming, vol. 2, no. 1, pp. 42–48, 2012.

[20] Chen TH, Wu CS. Efficient multi-secret image sharingbased on Boolean operations. Signal Processing";vol.91p.p.90–97, 2011.

[21] Abhishek Mishra and Ashutosh Gupta, Secret Sharing Scheme with Reversing, IEEE 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun (India), 4-5 September 2015 p.p.370-373.