Enhanced XOR-Based Progressive Visual Secret Sharing Using Multiple Decryptions

Vishal Singh Sachan, Mainejar Yadav and Ranvijay

Abstract This paper proposes XOR-based visual secret sharing rule using random grids with the abilities of OR as well as XOR-based visual cryptographic schemes. This scheme is different from previously proposed schemes as this paper proposes a lossless (k, n) threshold-based vcs with progressive recovery having advantages of multiple decryptions. Although previously proposed schemes were progressive with OR operator but in case of XOR their progressive nature was lost when the number of shares "t" is between "k" and "n", i.e., k < t < n. Our scheme overcomes this problem by proposing a truly progressive scheme, completely independent of the values of "k" and "n." In absence of a processing device the secret information can be simply reconstructed by OR-ing a threshold number of shares and in case, if a device having computational ability of XOR is available, then the secret information encoded is reconstructed lossless for (k, n) threshold, when all the "n" shares are collected. There is no pixel expansion, no requirement of codebook design and hence all the shares were generated of the same size of the original secret image.

Keywords Visual cryptography · Visual secret sharing · Random grids · Multiple decryptions

1 Introduction

Secret sharing is one of the most important cryptanalytic application. It is mainly employed in cases wherever the collaborating parties do not trust each other or they are unreliable whereas there is equal importance of the participants and thus the secret information is divided into parts and distributed among them in such a way that

V. S. Sachan (✉) · M. Yadav · Ranvijay
Computer Science and Engineering Department, MNNIT Allahabad, Allahabad, India
e-mail: er.singhvishal77@gmail.com

M. Yadav
e-mail: ruhulit1210@gmail.com

Ranvijay
e-mail: ranvijay@mnnit.ac.in

D. Dutta et al. (eds.), *Advances in VLSI, Communication, and Signal Processing*,
Lecture Notes in Electrical Engineering 587,
https://doi.org/10.1007/978-981-32-9775-3_84

individual shares of the participants reveal no original secret information, however, once a predefined number of participants group together their secret shares reveal the originally intended information. Shamir et al. [1] first introduced the idea of secret sharing, this scheme was mainly based on Lagrange Interpolation polynomial. In the present world, image security and secret sharing are one of the most important fields of work because the modification of digital image and using it for unlawful purposes has become very simple. Visual secret sharing scheme is a variant of cryptography that is based on the human visual system which performs the decoding phase and no further computation is needed. Hence it is simple and can be employed by everyone. Progressive scheme has a property that with the increase in number of shares the visual quality of the recovered image increases gradually, this is helpful when you have to assign some privilege based on the level of secret information they have.

Let us consider an example where "n" thieves are present, no one trusts each other therefore in order to gain low authorization access to the account a threshold number of shares are required whereas to perform high privileged operations an additional number of shares are needed. As additional shares are collected more authorization is granted.

This paper proposes an enhanced random grid-based progressive secret sharing algorithms with the abilities of both XOR and OR operations. Our scheme is truly progressive with both XOR and OR operations which were not there in previous schemes. Moreover, in our scheme when all the "n" shares are present we can reconstruct the secret information in a lossless manner provided that we are having a device with XOR operation and in absence of such device we can simply reconstruct by stacking the shares.

2 Related Work

There are several approaches that are proposed by different researchers. Naor and Shamir [2] first proposed the threshold-based VCS scheme. In their scheme "n" shares are generated corresponding to a secret image and each share does not reveal any information regarding the original secret key. These shares were then printed on "n" number of transparencies and given to the designated participants. This method was secure as each share do not reveal any information unless a "threshold number" of shares that is defined at the time of decoding are present. Kafri and Keren [3] in 1987 proposed the random grid model in which each of the shares that were generated is meaningless random grids and the size of the shares was identical to the original secret image, thus there was no pixel expansion. The decoding operation was same as that of traditional visual cryptography, by stacking both the encoded and the master grid original information can be reconstructed. The application of random grid in image encryption removes disadvantages such as pixel expansion, shape distortion, and codebook design. But due to the lack of encryption techniques to implement the (2, 2) technique to a more generalized (k, n) or (n, n) scheme, its application was mainly limited. Later in 2008 Chen and Tsao proposed (n, n) and

(2, n) [4] random grid-based visual secret sharing scheme, they extended the (2, 2) scheme so that more number of participants can participate and the algorithm can be applied to much wider areas. This scheme is then again extended by Chen and Tsao [5] to develop a more generalized and applicable (k, n) threshold-based scheme. In their scheme, a threshold number of shares was required at the decoding phase to reconstruct the original secret image and if that threshold "k" is not met then the secret image is not revealed.

The limitations of the above work done were that the recovered image was lossy, i.e., the key information was not fully recovered because of the monotonous property of OR operator, which degrades the visual appearance of the recovered secret information. To overcome this problem XOR-based VCS was introduced owing to its better quality image reconstruction ability, however, the XOR-based scheme would be useless if no suitable computational device having XOR operation is present. Thus in order to incorporate the advantages of both OR-based VCS scheme as well as XOR-based VCS theme, schemes having the property of both XOR as well as OR-based scheme was proposed. The multiple decryption ability is helpful in cases whenever a computational device with XOR functionality is not present then we can easily reconstruct a low visual quality secret image by performing OR operation(stacking) on the shares, thus revealing the secret information. Wu and Sun [6] proposed a (k, n) threshold-based scheme with abilities of multiple decryptions but the recovered image was lossy even when all the "n" shares were stacked. Yan et al. [7] later proposed a random grid-based vcs scheme having multiple decryptions with progressive recovery of secret image. By progressive recovery, we mean that as the number of shares increases the visual quality of reconstructed image also increases. When a device with XOR operation in not available, the secret information can be revealed by stacking "k" or more shares to generate the lossy secret image whereas when computational device having XOR operation is available then the secret image is lossily reconstructed if "k" shares are collected and lossless reconstructed when all "n" shares are collected.

3 Proposed Work

In this section, we will propose an enhanced XOR-based progressive visual secret sharing algorithm with the abilities of multiple decryptions. It is different from the previous schemes [7] as the previously proposed multiple decryption schemes were not truly progressive. The generation of shares is described in algorithm 1 whereas algorithm 2 describes the secret image recovery steps. Definitions required for proper understanding and implementation of the proposed algorithms is also given. This paper is organized into three sections, first the proposed algorithms then its performance analysis and finally experimental results and its comparison with previously proposed algorithms.

Algorithm 1. **The proposed scheme**

```
Input: A binary secret image SB and a colored cover image C both of same size MxN
and the threshold parameters (k, n).
Output: n meaningful shares $MS_1$, $MS_2$, $MS_3$, $MS_4$, $MS_n$ of size MxN
Step 1: for each position (x, y) of the secret image such that ($1 \le x \le M$, $1 \le y \le N$)
            repeat steps 2-7
Step 2: create $b_1$, $\overline{b_2}$ as follows
            $b_1 || \overline{b_2}$=Random_pixel (SB (i, j))
Step 3: create $b_2 \sim b_k$ as cipher pixels recursively using the following algorithm
        if (n >2)
        {
                For p=2 to k-1
                $b_p || \overline{b_{p+1}}$ =Random_pixel_generator (SB (i, j))
        }
Step 4: create $b_k$ as the last cipher grid pixel
                $b_k = \overline{b_k}$
Step 5: if n>k , set $b_{k+1}$ , $b_{k+2}$ , $b_{k+3}$ , $b_{k+4}$ ..... $b_n$ = 0
Step 6 : randomly rearrange $b_1$, $b_2$,…, $b_n$ to $c_1$, $c_2$, $c_3$…, $c_n$
Step 7: for each share $MS_i$ , $1 \le i \le n$
                do{
                    $MS_i$= C ;
            Randomly choose d ,d €{2,3}
            Then , MSi(i,j,d)=$c_i$
                        }
Step 8: Output n meaningful shares $MS_1$, $MS_2$, $MS_3$, $MS_4$ , … $MS_n$
```

Definition 1. **frandom ( )**

$$\text{frandom()} = \begin{cases} 0 \text{ with probability } 0.5 \\ 1 \text{ with probability } 0.5 \end{cases}$$

Definition 2. Random_pixel_generator (bs)

```
    Step 1.1 Create $b_k$ as a cipher-pixel
                $b_k$ = frandom( ),
    Step 1.2 Create $\overline{b_{k+1}}$ as follows
```

$$\overline{b_{k+1}} = \begin{cases} b_k & \text{if}(b_s=0) \\ \overline{b_k} & \text{if}(b_s=1) \end{cases}$$

```
Algorithm 2. The secret image recovery
Input: t meaningful shares $MS_1, MS_2, MS_3, MS_4, \ldots MS_t$ of size M X N, and the
    threshold parameter (k,n)
Output: A M x N binary secret image S’
Step 1: repeat steps 2 for each meaningful share $MS_t$
Step 2: for each position (x,y) of the secret image such that ($1\leq x \leq M$, $1 \leq y \leq N$)
        if( MSi(x,y,3)<2)
            $Ci(x,y)=MS_i(x,y,3)$
        else
            $Ci(x,y)=MS_i(x,y,2)$
Step 3: if a device having XOR operation is not available then stack all the shares
$C_1, C_2, C_3, \ldots C_n$ to recover the secret image S’, go to step 5 else goto step 4
Step 4: if computational device is present then simply XOR all the t shares, i.e.
        $S'=C_1\otimes C_2\otimes C_3\otimes C_4\ldots C_t$
Step 5: Output the binary secret image S’.
```

4 Performance Analysis of Proposed Algorithm

This section describes the performance analysis of the proposed algorithm by analyzing the security and performance metrics. We will analyze our algorithm based on various parameters and compare them with the previously proposed algorithms.

4.1 Definition (Average Light Transmission)

For a certain pixel “r” in a binary image SB whose size is M × N, the light transmission of a white pixel is defined as T(r) = 1; whereas, T(r) = 0 for “r” is a black pixel. Totally, the average light transmission of R is defined as follows:

$$\sum_{i=1}^{m}\sum_{j=1}^{n} T(SB(i, j)) \qquad (1)$$

4.2 Definition (Area Representation)

Let A (0) (resp. A(1)) represents the area of white (resp. black) pixels in binary secret image SB where A = A (0) ∪ A(1) and A (0) ∩ A(1) = ø. Hence the total area of all the corresponding white and black pixels will be SB (A (1)) and SB (A (0)), respectively, in image SB.

4.3 Definition (Contrast)

The contrast of the recovered secret image S' = $S_{S1} \otimes {}_{S2} \otimes S_{S3} \ldots\ldots \otimes S_{Sn}$ [SB(0)] with respect to the original binary secret image SB is defined as follows:

Let

$$t_1 = T(S_{S1} \otimes_{S2} \otimes S_{s3} \ldots\ldots.. \otimes S_{Sn}[SB(0)]$$
$$t_2 = T(S_{S1} \otimes_{S2} \otimes S_{s3} \ldots\ldots.. \otimes S_{Sn}[SB(1)]$$

Then,

$$\alpha = (t_1 - t_2)/(1 + t_2) \tag{2}$$

The contrast of the reconstructed secret image after OR or XOR operation must be greater than 0 so that the reconstructed secret information or image can easily be identified by the human visual system. Average light transmission is directly proportional to the contrast (α), so the value of contrast must be as high as possible, higher value means higher average light transmission which results in good quality reconstructed secret image.

4.4 Definition (Mean Squared Error (MSE))

Let us consider a binary secret image SB and S' be the recovered image both of dimensions MxN, then the mean squared error is the cumulative squared error between the original and the reconstructed image, lower value of MSE means lesser error. The mathematical formulae for calculating is as follows:

$$\text{MSE} = \frac{1}{MN} \sum_{i=1}^{m} \sum_{j=1}^{n} \left[SB(i, j) - S'(i, j) \right]^2 \tag{3}$$

4.5 Theorem 1. (Security)

There is no dependency among the bits $b_{1,}$ $b_{2,}$ b_3 … $b_{k\text{-}1}$ generated using the random pixel generator function and are also completely independent of the original secret binary image "SB." The bit b_k is dependent on the previous (k−1) bits generated and the original bit in the secret binary image due to the XOR operation being used in Step 4 and the remaining bits set b_{k+1}, b_{k+2}, b_{k+3} … b_n are generated using Step 5 of the algorithm 1. To make the scheme more secure cover image is used to hide the share bits that were generated b_1, b_2 … $b_{k,}$ b_{k+1} … $b_{n2,}$ $b_{n-1,}$ $b_{n.}$ Hence for t < k, the probability of secret image getting revealed is negligible, and XOR of shares less than "k" the probability of appearance of white as well as the black pixel is ½, i.e.,

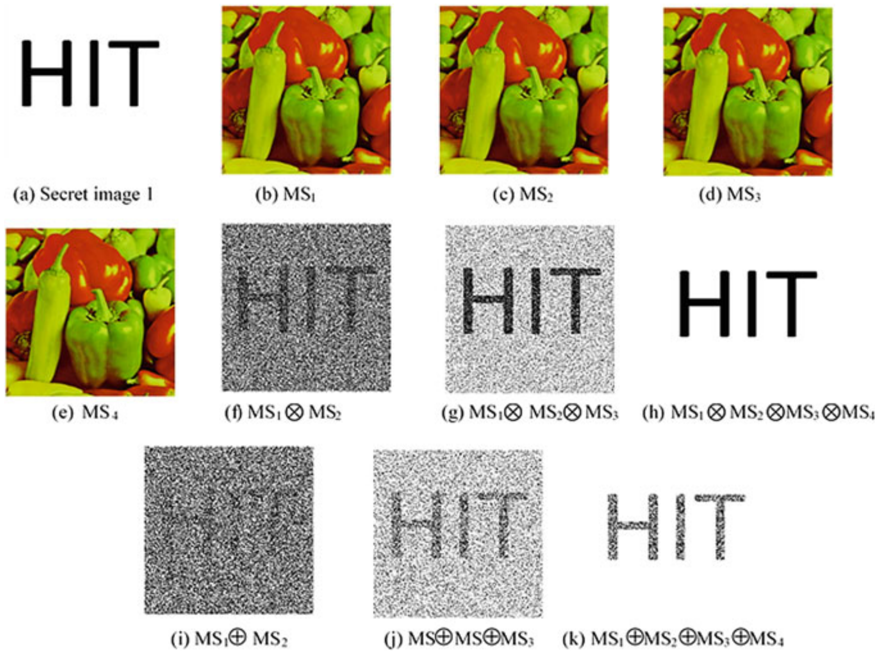
$$\begin{aligned}&T(S_{S1} \otimes_{S2} \otimes S3 \ldots\ldots.. \otimes S_{k-1}[SB(0)] = 0)\\&= T(S_{S1} \otimes_{S2} \otimes S3 \ldots\ldots.. \otimes S_{k-1}[SB(0)] = 1/2\end{aligned}$$

Thus each pixel which appears is not fixed as pixel placement is completely independent of each other due to the usage of flipping coin procedure and hence the proposed scheme is secure.

5 Experimental Results and Analysis

In this section we will perform experiments on different test secret images for different values of "k" and "n", analyze the performance metrics of the proposed algorithm and compare them with the previously proposed scheme [7] as well. In these experiments, all the images that were used are of size 512 × 512 pixels and all the experiments were carried out on Intel(R) Core(TM) i7-4790 CPU @3.60 GHz octa-core processor with 4 GB of RAM and Windows 10 Pro 64-bit operating system.

Figure 1(a) represents the secret image 1 used for simulation of the proposed scheme for (2, 4), Fig. 1(b–e) represents the shares generated MS_1, MS_2, MS_3, $MS_{4,}$ and Fig. 1(f–h) represents the results of XOR operation. The average light transmission and MSE values for t = 2, t = 3, and t = 4 are 0.00033, 0.40125, 1 and 0.48274, 0.24909, 0, respectively. Figure 1(i–k) represents the recovered images of OR operation. Figure 2(a) represents the secret image 2, Fig. 2(b–f) represents the meaningful shares that were generated, MS_1, MS_2, MS_3, MS_4, $MS_{5,}$ and Fig. 2(g–j) represents the result of XOR operation when k < = t < = n. The average light transmission and MSE values for t = 2, t = 3, t = 4, and t = 5 are 0.06344, 0.07018, 0.30920, 1 and 0.48513, 0.44905, 0.29954, 0, respectively. In a (3, 5) scheme when less than "k" shares are stacked no information is revealed about the original secret image and hence a threshold number of shares are always mandatory to reveal the original secret image. Figure 3(a) represents the secret image 3, Fig. 3(b–e) represents



(a) Secret image 1 (b) MS_1 (c) MS_2 (d) MS_3

(e) MS_4 (f) $MS_1 \otimes MS_2$ (g) $MS_1 \otimes MS_2 \otimes MS_3$ (h) $MS_1 \otimes MS_2 \otimes MS_3 \otimes MS_4$

(i) $MS_1 \oplus MS_2$ (j) $MS \oplus MS \oplus MS_3$ (k) $MS_1 \oplus MS_2 \oplus MS_3 \oplus MS_4$

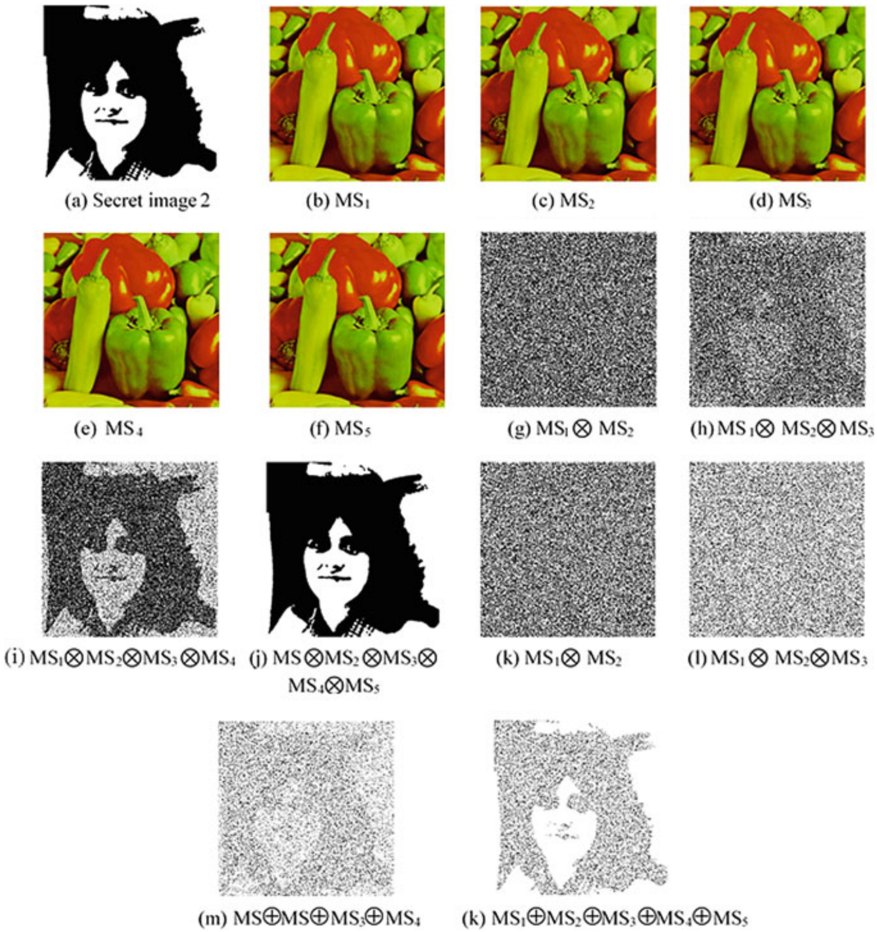
Fig. 1 Experimental results of proposed scheme for (2, 4) on secret image 1

the meaningful shares MS_1, MS_2, MS_3, $MS_{4,}$ and Fig. 3(f–h) represents the results of XOR operation when a different number of shares are present.

With more number of shares better reconstructed image is obtained and the image reconstructed for values of “t”, where “t” is k < t < n, the progressive nature is not lost and the proposed scheme behaves as true progressive in nature. The average light transmission and MSE values for t = 2, t = 3, and t = 4 are 0.00077, 0.39862, 1 and 0.432125, 0.25085, 0, respectively. As in a (2, 4) scheme, the average light transmission increases for t = 3 and does not decrease with increase in number of shares, i.e., for t = 4 & t = 5. Figure 3(i–k) represents the results of OR operation, the results obtained with XOR operation are truly progressive when the value of “t” lies between “k” and “n”, moreover, the visual quality obtained with XOR is more than the OR operator.

Figure 4(a) represents the secret image 4 and Fig. 4(b–f) represents the five meaningful shares MS_1, MS_2, MS_3, $MS_{4,}$ $MS_{5,\text{ and}}$ Fig. 4(g–j) represents the results of XOR operation when different number of shares are stacked. Figure 4(g) represents recovered image when t = 2, i.e., when two shares are present, Fig. 4(h–j) represents the recovered image with t = 3, t = 4 and t = 5, respectively. The average light transmission and MSE values for t = 2, t = 3, t = 4, and t = 5 are 0.12538, 0.14357, 0.50052,1 and 0.45384, 0.35032, 0.19983, 0, respectively.

From Table 1 it can be seen that in (2,4) case of previous scheme the average light transmission is increasing gradually with the increase in the number of shares “t”,



(a) Secret image 2 (b) MS_1 (c) MS_2 (d) MS_3

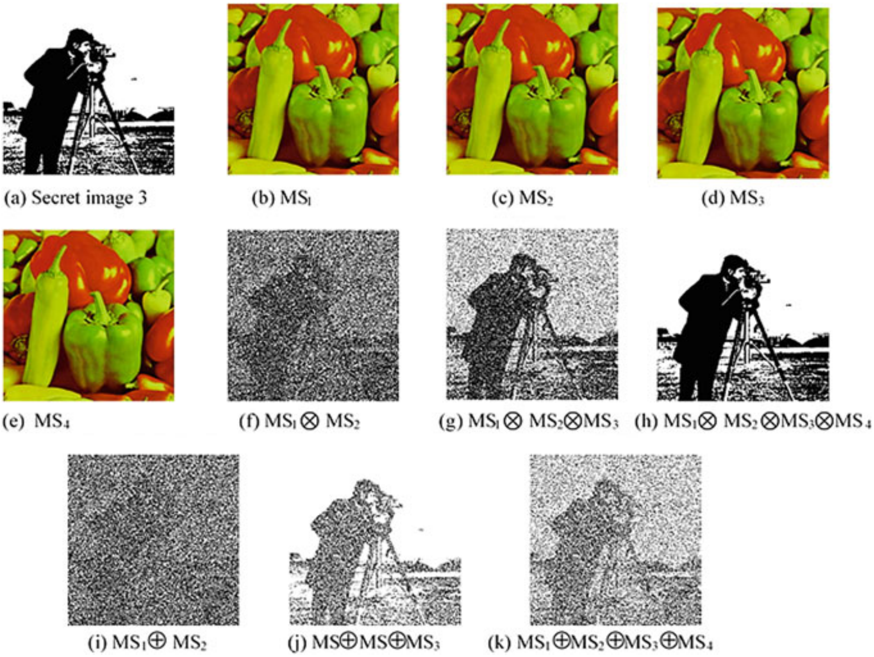
(e) MS_4 (f) MS_5 (g) $MS_1 \otimes MS_2$ (h) $MS_1 \otimes MS_2 \otimes MS_3$

(i) $MS_1 \otimes MS_2 \otimes MS_3 \otimes MS_4$ (j) $MS \otimes MS_2 \otimes MS_3 \otimes MS_4 \otimes MS_5$ (k) $MS_1 \otimes MS_2$ (l) $MS_1 \otimes MS_2 \otimes MS_3$

(m) $MS \oplus MS \oplus MS_3 \oplus MS_4$ (k) $MS_1 \oplus MS_2 \oplus MS_3 \oplus MS_4 \oplus MS_5$

Fig. 2 Experimental results of proposed scheme for (3, 5) on secret image 2

for t = 2 the value is 0.000607 which gradually increases to 0.002092 and then for t = 4 we get complete recovery, i.e., value becomes 1, in case of proposed scheme the value of average light transmission for t = 2, 3, 4 are 0.001293, 0.40079, and 1, respectively whereas comparing it with (2,5) case of previous scheme for t = 3 and t = 4 there is a gradual decrease in the average light transmission, i.e., for t = 3 the light transmission decreases to 0.06657 as compared to 0.06825 for t = 2 which further decreases to 0.001943 when t = 4 in spite of increase in the number of shares thereby violating the progressive nature. In contrast, the secret image in the proposed scheme is reconstructed progressively and the original information is not lost with the increase in the number of shares. There is progressive recovery and the average light transmission value increases with increase in the number of shares, i.e., for t = 2, 3, 4, and 5 the values are 0.12538, 0.143573, 0.50052, and 1, respectively.



(a) Secret image 3 (b) MS_1 (c) MS_2 (d) MS_3

(e) MS_4 (f) $MS_1 \otimes MS_2$ (g) $MS_1 \otimes MS_2 \otimes MS_3$ (h) $MS_1 \otimes MS_2 \otimes MS_3 \otimes MS_4$

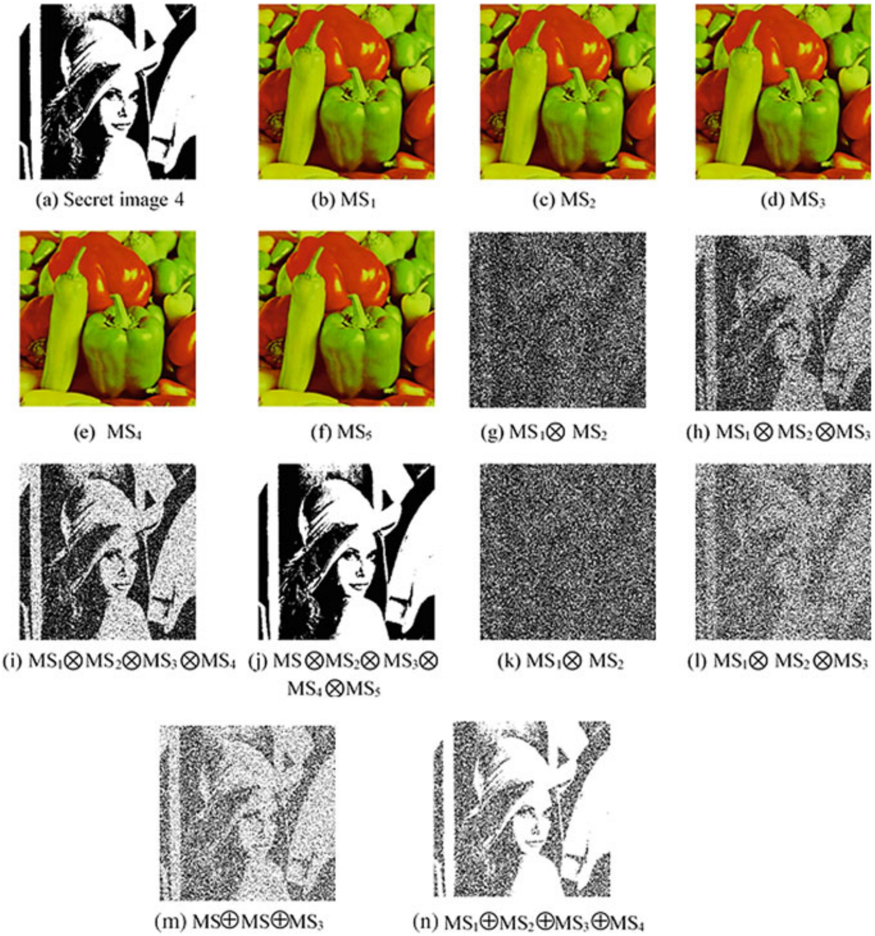
(i) $MS_1 \oplus MS_2$ (j) $MS \oplus MS \oplus MS_3$ (k) $MS_1 \oplus MS_2 \oplus MS_3 \oplus MS_4$

Fig. 3 Experimental results of proposed scheme for (2, 4) on secret image 3

When we compare both the cases of (2, 4) and (2, 5) we can easily infer that in case of the previous algorithm the progressive recovery is not always possible due to the self-complementing nature of the XOR operator. There might be cases where with XOR operator in spite of increasing the shares the quality of image degrades as demonstrated in (2,5) case, whereas in case of our scheme the nature of progressive recovery is always retained even for large values of n, though with the increase in the total number of participants the image recovery in more linear.

Table 2 lists the value of mean squared error of the proposed and the previous scheme for different values of k and n, lower the value of MSE higher is the quality of the image formed. Table 2 also supports the results drawn from Table 1, i.e., in some cases, previous algorithm loses the progressive nature with the increase in number of shares and the proposed algorithm overcome this problem. There might be also the case that in spite of increase in average light transmission the overall visual quality of the recovered image decreases which is also depicted by the MSE values. Table 3 lists the MSE values for recovered image with OR operation and it is evident that in the case of OR operation even when all the shares are present, secret image is not recovered completely.

In the case of OR operation even when all the shares are present, secret image is not recovered completely. The image reconstruction with OR operator is lossy and a low quality of image is formed.



(a) Secret image 4

(b) MS_1

(c) MS_2

(d) MS_3

(e) MS_4

(f) MS_5

(g) $MS_1 \otimes MS_2$

(h) $MS_1 \otimes MS_2 \otimes MS_3$

(i) $MS_1 \otimes MS_2 \otimes MS_3 \otimes MS_4$

(j) $MS \otimes MS_2 \otimes MS_3 \otimes MS_4 \otimes MS_5$

(k) $MS_1 \otimes MS_2$

(l) $MS_1 \otimes MS_2 \otimes MS_3$

(m) $MS \oplus MS \oplus MS_3$

(n) $MS_1 \oplus MS_2 \oplus MS_3 \oplus MS_4$

Fig. 4 Experimental results of proposed scheme for (2, 5) on secret image 4

Thus, for different values of “k” and “n” the secret image is completely recovered when t = n with XOR operation. Stacking also recovers the secret image but the recovery is lossy and complete information is not obtained. OR operator can be treated as a secondary option when a suitable device having the capability of performing XOR is not present so that a lower quality but visually recognizable version of the secret image can be easily constructed which is recognizable by the human visual system.

Figure 5(a) shows the performance of the proposed algorithm and previous algorithm [7] on secret image 1 for (2, 4). The graph is plotted between the average light transmission of each reconstructed image for different values of shares “t.” It can be seen that in each case the recovery in the proposed algorithm is strictly progressive and in case of a large number of shares, i.e., Fig. 5(b–c). The Fig. 5(b) represents the

Table 1 Average light transmission, of the proposed scheme and previous scheme [7] using XOR operation

	Proposed scheme				Previous scheme [7]			
(k, n)	t = 2	t = 3	t = 4	t = 5	t = 2	t = 3	t = 4	t = 5
(2,2)	1				1			
(2,3)	0.2533	1			0.2509	1		
(3,3)		1				1		
(2,4)	0.0014	0.4001	1		0.0006	0.0021	1	
(3,4)		0.1827	1			0.1823	1	
(4,4)			1				1	
(2,5)	0.1254	0.1436	0.5005	1	0.0683	0.0666	0.0019	1
(3,5)		0.0719	0.3086	1	–	0.068	0.0023	1
(4,5)			0.1433	1			0.1431	1
(5,5)				1				1

Table 2 Mean squared error of the proposed scheme and previous scheme [7] using XOR operation

MSE	Proposed scheme				Previous scheme [7]			
(k,n)	t = 2	t = 3	t = 4	t = 5	t = 2	t = 3	t = 4	t = 5
(2,2)	0				0			
(2,3)	0.3324	0			0.3326	0		
(3,3)		0				0		
(2,4)	0.4201	0.2500	0		0.4178	0.4987	0	
(3,4)		0.3754	0			0.3746	0	
(4,4)			0				0	
(2,5)	0.4539	0.3503	0.1998	0	0.4503	0.5028	0.4998	0
(3,5)		0.4476	0.2992	0		0.4508	0.4977	0
(4,5)			0.4004	0			0.399	0
(5,5)				0				0

plot for secret image 2 for (3, 5), Fig. 5(c–d) represents the plot for secret image 3 (2, 4), and secret image 4 (2, 5), respectively. From the graph, it is also evident that the performance of the proposed scheme is better than the previous scheme [7]. In case of the previous scheme [7] when number of shares increases more than “k” then there is a sharp decrease in the overall visual quality of the recovered image with XOR operation and the scheme does not behave as truly progressive in nature.

Table 3 MSE of proposed scheme and previous scheme [7] using OR operation

MSE	Proposed scheme				Previous scheme			
(k,n)	t = 2	t = 3	t = 4	t = 5	t = 2	t = 3	t = 4	t = 5
(2,2)	0.2439				0.2462			
(2,3)	0.4158	0.2447			0.4165	0.2452		
(3,3)		0.3682				0.3660		
(2,4)	0.4599	0.3718	0.2438		0.4550	0.4304	0.3669	
(3,4)		0.4617	0.3667			0.4624	0.3664	
(4,4)			0.4280				0.4276	
(2,5)	0.4772	0.4241	0.3452	0.2439	0.4709	0.4555	0.4545	0.4286
(3,5)		0.4825	0.4430	0.3665		0.4807	0.4658	0.4278
(4,5)			0.4792	0.4282			0.4791	0.4281
(5,5)				0.4584				0.4581

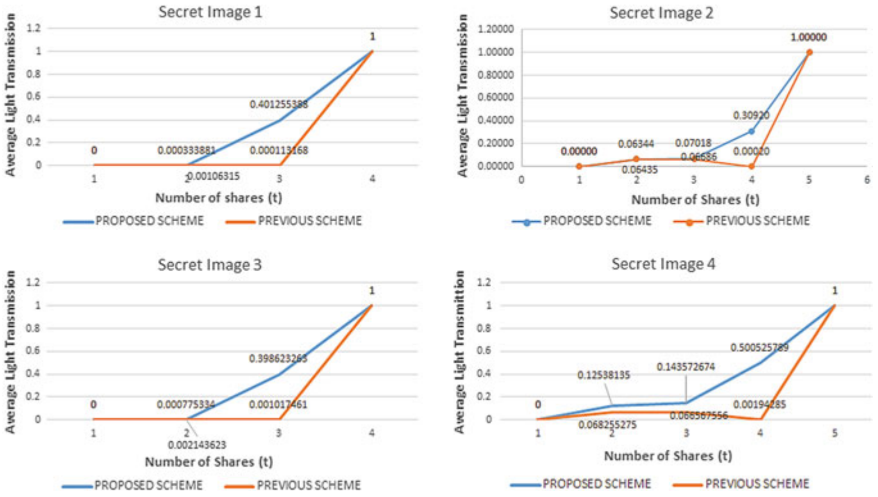


Fig. 5 Graphs showing the variation in average light transmission with different values of k and n

6 Conclusion

This paper proposes an enhanced random grid-based progressive secret sharing algorithms with the abilities of both XOR and OR operations. Our scheme is truly progressive with both XOR and OR operations which were not there in previous schemes. Moreover, in our scheme when a computational device having XOR operation is present then we can recover our lossless secret image when all the shares are present and in absence of such device, we can recover secret information by simply stacking the shares. In comparison with other schemes, there is no pixel expansion and basis matrix requirement for the share generation phase as the shares generated are meaningful and it appears to the intruder that the shares are not carrying any information, hence it is more secure. The experimental results demonstrate the capability of our scheme and it can be applied to a variety of real-time applications as well. Comparison with previous schemes reveals that our scheme has several benefits that were lacking in previous schemes.

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
2. Naor, M., Shamir, A.: Visual cryptography, Advances in Cryptography. In: EUROCRYPT 94, LNCS, vol. 950, pp. 1–12 (1994, 1995)
3. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Opt. Lett. **12**(6), 377–379 (1987)
4. Chen, T.H., Tsao, K.H.: Visual secret sharing by random grids revisited. Pattern Recognit. **42**(11), 2203–2217 (2009)
5. Chen, T.-H., Tsao, K.-H.: Threshold visual secret sharing by random grids. J. Syst. Softw. **84**(7), 1197–1208 (2011)
6. Wu, X., Sun, W.: Random grid-based visual secret sharing with abilities of OR and XOR decryptions. J. Vis. Commun. Image Represent. **24**(1), 48–62 (2013)
7. Yan, X., Wang, S., Niu, X., Yang, C.N.: Random grid-based visual secret sharing with multiple decryptions. J. Vis. Commun. Image Represent. **26**, 94–104 (2015)