Journal of Artificial Intelligence and Data Mining (JAIDM), Vol. 11, No. 2, 2023, 195-211.

Shahrood University of Technology

Journal of Artificial Intelligence and Data Mining (JAIDM)
Journal homepage: http://jad.shahroodut.ac.ir

Research paper

A New Scheme for Lossless Meaningful Visual Secret Sharing by using XOR Properties

Zeinab Mehrnahad[1], AliMohammad Latif[1*] and Jamal Zarepour Ahmadabadi[2]

1. Department of Computer Eengineering, Yazd University, Yazd, Iran.
2. Department of Computer Science, Yazd University, Yazd, Iran.

Article Info

Article History:
Received 19 December 2022
Revised 31 January 2023
Accepted 07 March 2023

DOI:10.22044/jadm.2023.12460.2395

Keywords:
Meaningful secret sharing, Secret sharing, Visual secret sharing, Genetic algorithm.

**Corresponding author: alatif@yazd.ac.ir (A.Latif).*

Abstract

In this work, a novel scheme for lossless meaningful visual secret sharing using XOR properties is presented. In the first step, genetic algorithm with an appropriate proposed objective function create noisy share images. These images do not contain any information about the input secret image, and the secret image is fully recovered by stacking them together. Because of attacks on image transmission, a new approach for construction of meaningful shares by the properties of XOR is proposed. In recovery scheme, the input secret image is fully recovered by an efficient XOR operation. The proposed method is evaluated using the PSNR, MSE, and BCR criteria. The experimental results present good outcome compared with other methods in both quality of share images and recovered image.

1. Introduction

Despite of advantages of using the Internet and data sharing via it, security in communications is an important issue. Protecting information such as political, military and commercial information, and ensuring their privacy is the highest priority [1, 2]. Traditional techniques such as cryptography and steganography protect information from malicious users. cryptography converts a secret into an unreadable format and the recipient can decode it using encryption keys. Steganography hides the message in the form of appropriate cover files so that it cannot be detected. In both above methods, information is stored in an encrypted file, so it may be lost or damaged [3]. Secret sharing is proposed to solve this problem. The secret sharing scheme, which is called (k, n) threshold secret sharing, was introduced in the late 1970s by Shamir [4]. The secret S is converted into n shares such as $R_1.R_2.\ldots.R_n$ and distributed among n participants.

To recover the secret, any t ($R_1.R_2.\ldots.R_t$, $k \leq t \leq n$) shares can do it and with k -1 or fewer shares, secret information cannot be recovered [5]. The recovery phase of secret sharing method has a high computational cost and is time-consuming. Some secret sharing schemes are based on Shamir's method and have complex computation in the recovery phase [6- 10].

Visual Secret Sharing (VSS) was introduced by Naor and Shamir to reduce the recovery cost of secret sharing [11]. In VSS, n meaningless shares are constructed. Then, the secret image can be recovered by stacking shares by human visual system. In some applications secrete image can be recovered using simple computations such as OR/XOR operation. An approach, (2, 2) Naor and Shamir's visual secret sharing, is shown in Table 1.

Table 1. Naor and Shamir's secret sharing method [12].

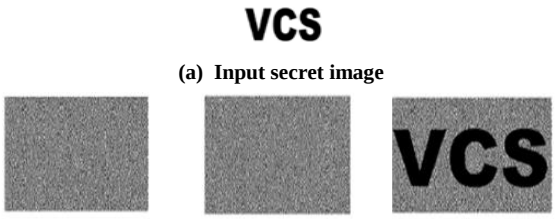
pixel S(i,j)	probability	Share R1	Share R2	R1+R2
	0.5			
	0.5			
	0.5			
	0.5			

According to this table, each pixel (column 1) is converted into one of the 4 sub-pixels in each share (columns 3 & 4) with a probability of 0.5. As it can be seen, black pixels are recovered 100% and white pixels are recovered 50% [12].
In Naor's scheme, a codebook is first created and then shares are constructed using this codebook.
All types of possible codebooks are shown in Figure 1. It should be noted that any of these codebooks can be used to create shares [13].

(a) vertical **(b) horizontal** **(c) diagonal**

Figure 1. Types of codebooks for visual secret sharing [13].

The advantages of VSS schemes that have attracted attention in the recent years are the alternative arrangement of share images and their simple recovery. Disadvantage of the schemes based on naor's scheme are using codebook and having pixel expansion [14, 15]. An example of a (2, 2) visual secret sharing is shown in Figure 2. Based on this figure, the size of share images and recovered image are twice of secret image. Therefore, the researchers provided some solutions to solve pixel expansion which one of them was Random Grid (RG) [16].



(a) Input secret image

(b) share R1 **(c) Share R2** **(d) Share R3**

Figure 2. A (2, 2) Naor's visual secret sharing.

VSS scheme based on RG was presented by Kafri and Keren. They proposed three different algorithms to encrypt a binary image into several shares [16]. As shown below, these algorithms receive the input image B and generate two random images R_1 and R_2 that do not have any information of the secret image. The secret B is revealed by stacking R_1 and R_2. The size of shares is the same as the input secret image. The recovery procedure is the same as the traditional VSS.

Algorithm 1

Generate R1 as a random grid, $T(R_1) = 1/2$
// for (each pixel R_1[i, j], 1≤i≤w and 1≤j≤h) do
// R_1[i, j] = random_pixel (0,1)
for (each pixel B [i, j] 1≤i≤w and 1≤j≤h) do
{if (B [i, j] = 0) R2[i, j] = R1[i, j]
else R_2[i, j] = R_1[i, j]}
Output (R1,R2)

Algorithm 2

Generate R1 as a random grid, $T(R_1) = 1/2$
for (each pixel B [i, j] 1≤i≤w and 1≤j≤h) do
{if (B[i, j] = 0) R2[i,j] = R1[i,j]
else R_2[i, j] = random_pixel (0,1)}
Output (R1,R2)

Algorithm 3

Generate R1 as a random grid, $T(R_1) = 1/2$
for (each pixel B [i, j] 1≤i≤w and 1≤j≤h) do
{if (B [i, j] = 0) R2[i,j] = random_pixel (0,1)
else R_2[i, j] = R_1[i, j]}
Output (R1,R2)

After that some schemes were presented based on RG that have advantages such as no pixel expansion and having no codebook. However, disadvantages of these schemes is low contrast of recovered secret image [17 - 20].
To enhance the visual quality of recovered images, XOR operation is used between shares to recover the secret image. Also at the recovery phase of VSS schemes by human visual system, we need full alignment of the transparent shares. This procedure is not easy in practice even for the experienced participant. If a little movement occurs in a few pixels of the share images, the recovery cannot be occurred. The VSS schemes based on XOR recovery solve the problems of the requirement of alignment in the decryption phase and complex computation [21-23].
In 2007, Wang et al. presented a method for visual secret sharing using Boolean operations [24]. In their method, according to the input secret image S and the number of shares which is n, n + 1 random matrices is generated ($B_1 . \ldots . B_{n+1}$). Then n intermediate matrices are created as $C_i = B_i \& S$, $1 \leq i \leq n$, which & stands for AND operation. By using intermediate matrices, shares are generated with the relation $R_i = B_{n+1} \oplus C_i . 1 \leq i \leq n$. Their method does not have pixel expansion, However, the shares are noise-like and meaningless. Encryption is executed with XOR and is performed by $R_s = R_i \oplus R_j . i \neq j$. This method has no pixel expansion, and the quality of recovered image is good but the shares are still noisy. Due to the fact that noisy images are not safe and attract the attention of malicious in the transmission of information, some methods were presented so that share images are meaningful while not having any information from the input secret image.
In 2015, Ou *et al*. presented a meaningful VSS method [25]. Their algorithm is implemented in three steps. In the first step, according to the number of shares n, a matrix with numbers 0 to $2^n - 1$ is created in binary. Then this matrix is divided into two matrices M_n^{odd} and M_n^{even} based on the Hamming weight. The Hamming weight of

a binary string is sum of ones in the string. For example, hamming weight in A = 0 1 0 1 0 0 1 is H(A) = 3.

Example 1.

For more clarity, the construction of M_n^{odd} and M_n^{even} for n = 2 is shown.

$$n = 2 \Longrightarrow M_n = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$M_n^{odd} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} . \; M_n^{even} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$$

In the second step, n matrices of shares $R_1 . R_2 . \ldots . R_n$ are generated that have the same size as the secret image. After that, a row of M_n^{odd} or M_n^{even} is selected for each pixel of the input secret image randomly. Then each bit of it is placed into the matrices corresponding to shares.

Suppose n = 2, the values of pixels of each share per one pixel of input secret image, S (i, j), are determined according to (1) and (2). The r is a random integer number, which is equivalent to the row number of the matrix M.

$$R_1(i,j) = \begin{cases} M_n^{even}(r,1) & if \;\; S(i,j) = 0 \\ M_n^{odd}(r,1) & if \;\; S(i,j) = 1 \end{cases} \quad (1)$$

$$R_2(i,j) = \begin{cases} M_n^{even}(r,2) & if \;\; S(i,j) = 0 \\ M_n^{odd}(r,2) & if \;\; S(i,j) = 1 \end{cases} \quad (2)$$

In the third step, a cover image of the same size as the secret image is given as input. At this step, some pixels are randomly selected from the cover image and placed in the matrix of share images.

In 2020, Mohan introduced a new version of the method presented by Duanho [26]. The advantages of this scheme is no pixel expansion and satisfied quality due to recovering by XOR operation. Disadvantages are that it is applicable for binary images and recovered image is not 100% recovered.

In 2019, Chiu *et al*. proposed two progressive visual cryptography models that adopt a common encryption process. [23] The method uses a binary image as the input secret image and n binary images as cover images C_i, $1 \leq i \leq n$. There are n meaningful shares R_j, $1 \leq j \leq n$ in output. To encrypt white and black pixels of input secret image, two main codebooks M_b and M_w are introduced, respectively. The embedding codebooks E_b and E_w are used to embed black and white pixels of cover images into shares.

The elements of M_b / M_w and E_b / E_w codebooks are n-tuple column vectors. This method does not have the problem of pixel expansion because each secret pixel and cover pixel are encrypted by one n-tuple column vector, but still, it uses codebooks. The scheme has lossless recovery and applies to binary images. To use for grayscale images, firstly an input image is processed by halftone techniques and so the quality of the input image decrease before encryption [27, 28]. The limitation of this scheme is that it is applicable for number of shares $n \geq 4$ and if n < 4 it is not lossless anymore.

In 2021, Wang *et al*. proposed an AMBTC-based visual secret sharing with meaningful shares [29]. AMBTC is a lossy data compression algorithm for gray images. Their method consists of three phase: compression, sharing, recovery phase. At first phase they use AMBTC compression before secret sharing to reduce the amount of information in transition. The secret image and n cover images are compressed to generate high and low quantization levels and bitmaps. In sharing phase, for each pixel of secret image bitmap, randomly choose k images from n cover images. If the XOR result of k images' $BM_{i,j}$ (bitmap of position i,j) is equal to the secret image $BM_{i,j}$, do nothing and if is not equal randomly chose one of the k cover images and flip $BM_{i,j}$ of this image. In this method pixel expansion is solved but the recovered image is not lossless and has low quality.

In 2022, Zhao *et al*. introduced a (k, n) visual cryptography scheme based on RG and Boolean operations [30]. In their method, according to each pixel of input secret image S (i, j) and the number of shares, steps 1-4 are repeated until shares $R_1 . R_2 . \ldots . R_n$ are generated.

1) Generate k − 1 pixels randomly by 0 and 1: $r_1 . r_2 . \ldots . r_{k-1}$.
2) Compute $r_k = S(i.j) \oplus r_1 \oplus r_2 \oplus \ldots \oplus r_{k-1}$.
3) Let $r_{k+1} = r_{k+2} = \ldots = r_n = 0$.
4) Assign $r_1 . r_2 . \ldots . r_n$ to $R_1(i.j) . R_2(i.j) . \ldots . R_n(i.j)$ randomly.

Despite of their method have no pixel expansion but the shares are noise-like and meaningless. Recover the secret image occurred by stacking t ($t \geq k$) shares with OR operation.

Some challenges in the existing schemes for visual secret sharing are presented as follows.

1- Some schemes suffered from the problem of pixel expansion. Because each pixel of input secret image converts to m pixels in the share, so the share is m times larger than the input secret image [31, 32].

2- The introduced methods were applicable for binary images and include a method to encode black and white pixels. For gray images, it is necessary to apply halftone algorithms so that they can be converted into a binary image and then secret sharing can be done [25, 26, 28, 33].

3- Another problem of visual secret sharing is the low contrast of the recovered image. New methods were introduced to increase the quality of recovery images using XOR. These schemes have good contrast and require few and insignificant computations [31, 32, 34, 35, 36].
4-In some existing schemes shares are noise-like so attract the attention of malicious users. Managing several noise-like images and distinguishing between them is also difficult. If some of noise-like shares were mixed up by mistake, this will cause difficulties in the recovery [22, 24, 36, 37].
overall, the challenges mentioned above are the limitations of the existing methods. The existing schemes proposed methods to fix or improve some of them, but not all cases were fixed together. In our proposed method we tried to solve all the mentioned limitations, including no pixel expansion, applying for gray images, lossless recovery of secret image and meaningful share images. We make some improvements such as quality of share images. In this paper, a novel for lossless meaningful visual secret sharing based on XOR properties is introduced. XOR operation has properties that can be used to generate meaningful shares for lossless recovery. These features are explained in the next section. The proposed scheme has no pixel expansion and shares are meaningful. It applies to gray level images without halftone algorithm. We construct the noise-like shares using genetic algorithm and XOR properties. The secret image will be completely recovered by stacking them. In the next step, the cover image is used to generate meaningful shares. In the recovery phase, the input secret image with lossless recovery is achieved by XOR.
The rest of the paper is organized as follows. Section 2 contains the preliminaries that is used in this paper and related papers to meaningful visual secret sharing. Section 3 contains our proposed method. Experimental results are described in Section 4, and Section 5 contains the conclusions.

2. Preliminaries

A brief overview of concept of visual secret sharing, meaningful visual secret sharing and XOR properties are discussed in the following sections. In this paper, $\otimes$ is used for OR operation, $\oplus$ is used for XOR operation, and & is used for AND operation.

2.1. XOR properties

In this section, some properties of the XOR operation are briefly defined [37, 38]. If A and B are binary numbers, the operation $\oplus$ satisfies the following conditions:

Table 2. Some properties of XOR.

1	$\boldsymbol{A} \oplus \boldsymbol{B} = (\boldsymbol{A}'\&\boldsymbol{B}) \otimes (\boldsymbol{B}'\&\boldsymbol{A})$
2	$\boldsymbol{A} \oplus \boldsymbol{B} = \boldsymbol{B} \oplus \boldsymbol{A}$
3	$\boldsymbol{A} \oplus \boldsymbol{0} = \boldsymbol{A}$
4	$\boldsymbol{A} \oplus \boldsymbol{1} = \boldsymbol{A}'$
5	numbers of 1 is odd $\Rightarrow \boldsymbol{0} \oplus \boldsymbol{1} = \boldsymbol{1}$
6	numbers of 1 is even $\Rightarrow \boldsymbol{0} \oplus \boldsymbol{1} \oplus \boldsymbol{1} = \boldsymbol{0}$
7	numbers of A is even $\Rightarrow A \oplus A \oplus A \ldots \oplus A = 0$
8	numbers of A is odd $\Rightarrow A \oplus A \ldots \oplus A = \mathrm{A}$

2.2. Visual secret sharing

In a (k, n) visual secret sharing, two matrices such as M_0 and M_1 with size m × n are made to encode black and white pixels, in which n is the number of shares. Two matrices must have the following properties for secret sharing to be efficient [40, 41].

1) If we call the vector obtained by stacking any k rows out of n rows in matrix M_0 as V_0 and k rows out of n rows in matrix M_1 as V_1 .
It should be $H(V_0) < H(V_1)$ where H(V) is hamming weight function.

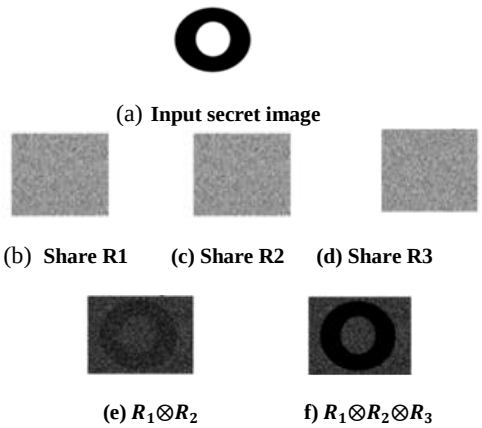
2) By placing i rows that $1 \leq i < k$, we have:
$H(V_0) = H(V_1)$.

Condition 1 checkouts the contrast of the recovered image and condition 2 satisfies security of VSS.

Example 2.
The following two matrices have above conditions for a (3, 4) visual secret sharing.

$$M_0 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}. \; M_1 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

If the secret image appears gradually by stacking k shares or more, it is called progressive visual secret sharing. In progressive visual secret sharing by stacking more shares, the secret image can be recovered with higher quality. In other words, by increasing the number of shares, the resolution of the recovered image can be increased [23].
An example of progressive visual secret sharing (2,3) is shown in the Figure 3.
The input secret image is shown in part (a) and shares are shown in parts (b-d). In part (e) shares R_1 and R_2 are stacked together and secret image is recovered. In part (f), by stacking shares R_1, R_2 and R_3, secret image is recovered with higher quality.



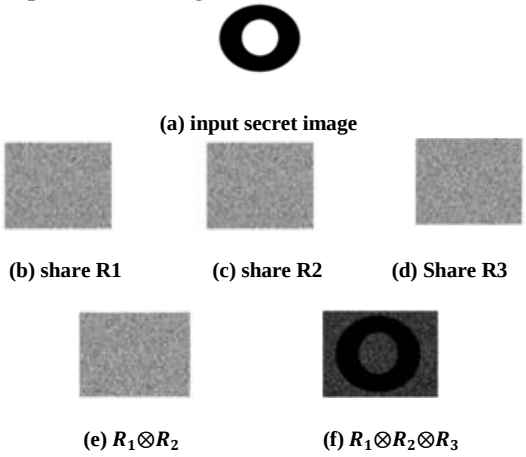
(a) **Input secret image**

(b) **Share R1** **(c) Share R2** **(d) Share R3**

(e) $R_1 \otimes R_2$ **f)** $R_1 \otimes R_2 \otimes R_3$

Figure 3. Progressive visual secret sharing [23].

If all shares must be available to retrieve the secret image, it is called (n, n) visual secret sharing [42]. In this case, if only one share is not available, it is not possible to recover the secret image. An example of (n, n) visual secret sharing is shown in Figure 4. In part (a), the input secret image is shown and shares are shown in parts (b-d). In part (e) shares R1 and R2 are stacked together. In part (f), by stacking shares R_1, R_2 and R_3, input secret image is recovered.



(a) input secret image

(b) share R1 **(c) share R2** **(d) Share R3**

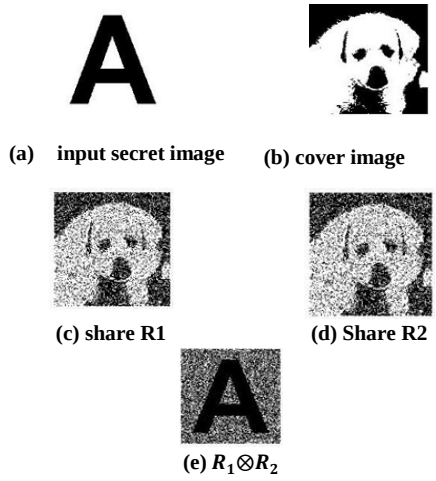
(e) $R_1 \otimes R_2$ **(f)** $R_1 \otimes R_2 \otimes R_3$

Figure 4. A (3, 3) visual secret sharing.

2.3. Meaningful visual secret sharing

In meaningful visual secret sharing, the shares are no longer random and meaningless and have a special meaning. This method is also called user-friendly visual secret sharing. One of the advantages is that meaningful shares do not attract the attention of disturbing entities to attack and can have better security [43,44].

Figure 5 shows an example of a meaningful visual secret sharing method. The input secret image is shown in part (a) and the cover image is shown in part (b). In parts (c) and (d), shares are meaningful and show the cover image. In part (e), by stacking two shares, secret image is recovered.



(a) input secret image **(b) cover image**

(c) share R1 **(d) Share R2**

(e) $R_1 \otimes R_2$

Figure 5. A meaningful visual secret sharing.

In the following, some concepts related to meaningful visual secret sharing are introduced [22, 25].

1) Average light transmission

The light transmission of pixel p in image S with size H × W is the probability that pixel p is white. It is shown as T(p). For a white pixel, the light transmission is T(p) = 1 and for a black pixel is T(p) = 0. Therefore, average light transmission for image S is defined as follows.

$$T(s) = \frac{\sum_{i=1}^{H} \sum_{j=1}^{W} T_s(i, j)}{H \times W} \quad (3)$$

2) Area representation

Consider W [0] is the range of all white pixels in image A and W [1] is the range of all black pixels in image A, so that W = W (1) ∪ W (0) and W (1) ∩ W (0) = 0. S [W [0]] and S [W [1]] are the corresponding range of all black and white pixels in image S.

3) Contrast of recovered secret image

The recovered image of n shares $R_1.R_2.\ldots.R_n$ is $R_s = R_1 \oplus R_2 \oplus \ldots \oplus R_n$. The contrast of R_s for input secret image S is:

$$\alpha_{Rs} = \frac{T(R_s[S[1]]) - T(R_s[S[0]])}{1 + T(R_s[S[0]])} \quad (4)$$

The range of α_{Rs} is [0,1]. For $\alpha_{Rs} > 0$, the recovered secret image with XOR can show the information of the secret image. The contrast criterion is used to measure the quality of the recovered secret image.

4) Contrast of share

Similar to the contrast of the recovered image, the contrast of share is defined as follows. The contrast of the share R_i concerning cover image C is:

$$\alpha_{Rs} = \frac{T(R_i[C[1]]) - T(R_i[C[0]])}{1 + T(R_i[C[0]])} \quad (5)$$

For $\alpha > 0$, the share image can display the information of the cover image. If $\alpha = 0$, the share is noisy and meaningless.

5) Security

In visual secret sharing (k, n), if the following condition is satisfied for k shares ($1 \le k < n$), the secret sharing is secure:

$$T(R_s[S[1]]) = T(R_s[S[0]]) \quad (6)$$

where $R_s = R_1 \oplus R_2 \oplus ... \oplus R_k$, $1 \le k < n$

6) Lossless recovery

If $\alpha_{Rs} = 1$, the scheme is lossless recovery. lossless means that all information of input secret S could be recognized in recover image R_s.

7) Genetic algorithm

The genetic algorithm (GA) is a search heuristic algorithm that is used to solve optimization problems by using mutation, cross-over, and selection operators.

GA starts from a set of random solutions and seeks to find the optimal solution with the objective function that is defined by user. The candidate solutions are called population. Each population consists of a number of chromosomes. The algorithm tries to reach the optimal solution by performing mutation and cross-over on chromosomes. For more information about GA, you can see [45].

3. Proposed meaningful VSS scheme

The proposed method consists of two steps. The first step generates noise-like images and the second step generates meaningful share images. In this method, properties of the XOR are used to generate share images. In the following, each step is explained separately. It should be noted that image recovery is obtained by applying OR and XOR on share images. The recovery phase is described in Section 3-3.

3.1. Construct meaningless share images

In our proposed method to achieve full recovery of input secrete image, two matrices M_0 and M_1 must be defined that black pixels in the secret image are become zero, and white pixels are become one in the recovered image. According to 5th and 6th properties in Table 1, one example of two matrices M_0 and M_1 are defined as follows. The XOR-ed result of zeros and ones in each row of the matrix M_0 is zero. Also it is one for matrix M_1.

$$M_0 = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

$$\text{Row1} = 0 \oplus 0 \oplus 0 = 0$$
$$\text{Row2} = 1 \oplus 1 \oplus 0 = 0$$

$$M_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\text{Row1} = 1 \oplus 0 \oplus 0 = 1$$
$$\text{Row2} = 1 \oplus 1 \oplus 1 = 1$$

Considering that the number of states of matrix M increases exponentially with the increase of n, so in this study, we try to obtain M_0 and M_1 by GA. To generate n shares, the matrix M with size $2^n \times n$ includes different combinations of ones and zeros. Then this matrix is separated to M_0 and M_1. By definition of suitable cost function, the best permutation is achieved by GA.

3.1.1. Our proposed GA

The parameters of our GA are given in Table 3. npop shows the number of the initial population, Pc is the cross-over rate, and Pm is the mutation rate. By using Pc, the number of crossover (ncross) and by using Pm, the number of mutations (nmut) is determined.

Table 3. Hyperparameters of proposed GA.

Cross-over	Two point cross-over
mutation	Random uniform
Npop	20
Pc	0.6
Pm	0.1

The fundamental of proposed method is algorithm 4 that is used in the proposed GA. Algorithm 5 is GA that is used to generate meaningless shares.

Algorithm 4

Input: Matrix M_0, M_1, input secret image S

Output: Meaningless shares $R_1, R_2, \ldots, R_n$

for each pixel in secret image S as S (i, j) with size H × W that $1 \le i \le H$, $1 \le j \le W$, do

1) If S (i, j) = 0 select random row in M_0 and insert in shares $R_1(i, j), R_2(i, j), \ldots, R_n(i, j)$

2) If S (i, j) = 1 select random row in M_1 and insert in shares $R_1(i, j), R_2(i, j), \ldots, R_n(i, j)$

end for

Example 3.

let S (1, 1) = 0, and the first row of the matrix M_0 is selected. Values are placed in the matrices of shares as follows for the number of shares n = 3.

$$M_0 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

$$R_1 = \begin{bmatrix} 0 & - & - \\ - & - & - \\ - & - & - \end{bmatrix} \; R_2 = \begin{bmatrix} 1 & - & - \\ - & - & - \\ - & - & - \end{bmatrix} \; R_3 = \begin{bmatrix} 0 & - & - \\ - & - & - \\ - & - & - \end{bmatrix}$$

Algorithm 5

Input: Parameters of GA, input secret image S, numbers of shares n

Output: The meaningless share images $\boldsymbol{r_1}.\boldsymbol{r_2}.\ldots.\boldsymbol{r_n}$, the restored image Rs

1) Initial population is generated as follows.
- A $2^n \times n$ matrix M is generated with 0 & 1.
- Divide Matrix M into two matrices M_0 and M_1.

2) For each chromosome in the population
- Algorithm 1 is executed.
- The cost function is applied on the restored image Rs

3) The values of the cost function are sorted in ascending order.

4) Cross-over is applied on the chromosomes to create new chromosomes.

5) Mutation is applied on the chromosomes to create new chromosomes.

6) (npop + ncross + nmut) chromosomes are sorted in ascending order. npop of the best of them are selected as new population.

7) Steps 2 to 6 are repeated until the value of the cost function becomes zero.

8) By the best answer the share images are generated.

3.1.2. Cost function

In the proposed scheme, if M_0 and M_1 are generated correctly, the share images are noise-like and the recovered image is fully restored. We use Bit Error Rate (BER) in the cost function. The value of BER between the recovered image and the input secret image is calculated in each iteration of GA. The algorithm continues until the BER between the input secret image and the recovered image becomes zero. The BER between two images f and g with size H × W is calculated according to (7) [36].

$$BER = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} f(i,j) \oplus g(i,j)}{H \times W} \quad (7)$$

Algorithm 6: Cost function

Input: Secret image S, restored image Rs

Output: The value of the BER

According to Equation (7), the BER value is calculated as follows:

F1 = BER value of the input secret image and the restored image

Cost = F1

Figure 7 shows the different states of generated share images and the recovered image with different matrices M_0 and M_1. As you can see in part (a), the secret image can be seen in the shares. Also recovered image is not fully restored. In part (b) the recovered image is not fully restored. In part (c) shares are noise-like but the recovered image is not restored and is noise-like too. In part (d), conditions are satisfied. Shares are noise-like, and as you can see, the recovered image is fully restored.

For more clarity the diagram of step 1 for constructing meaningless shares is shown in figure 6.

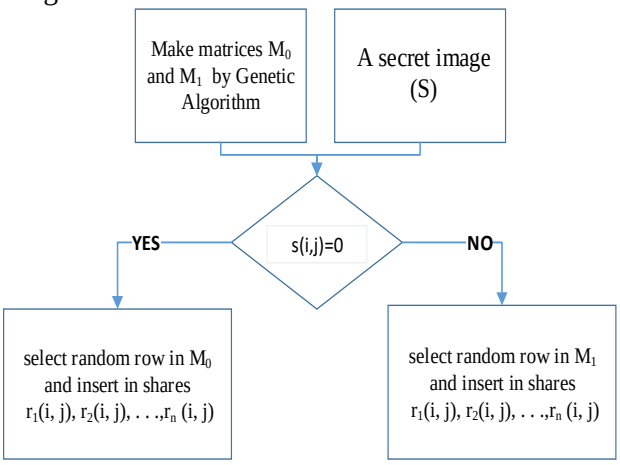


Figure 6. Diagram of constructing meaningless shares.

3.2. Construct meaningful share images

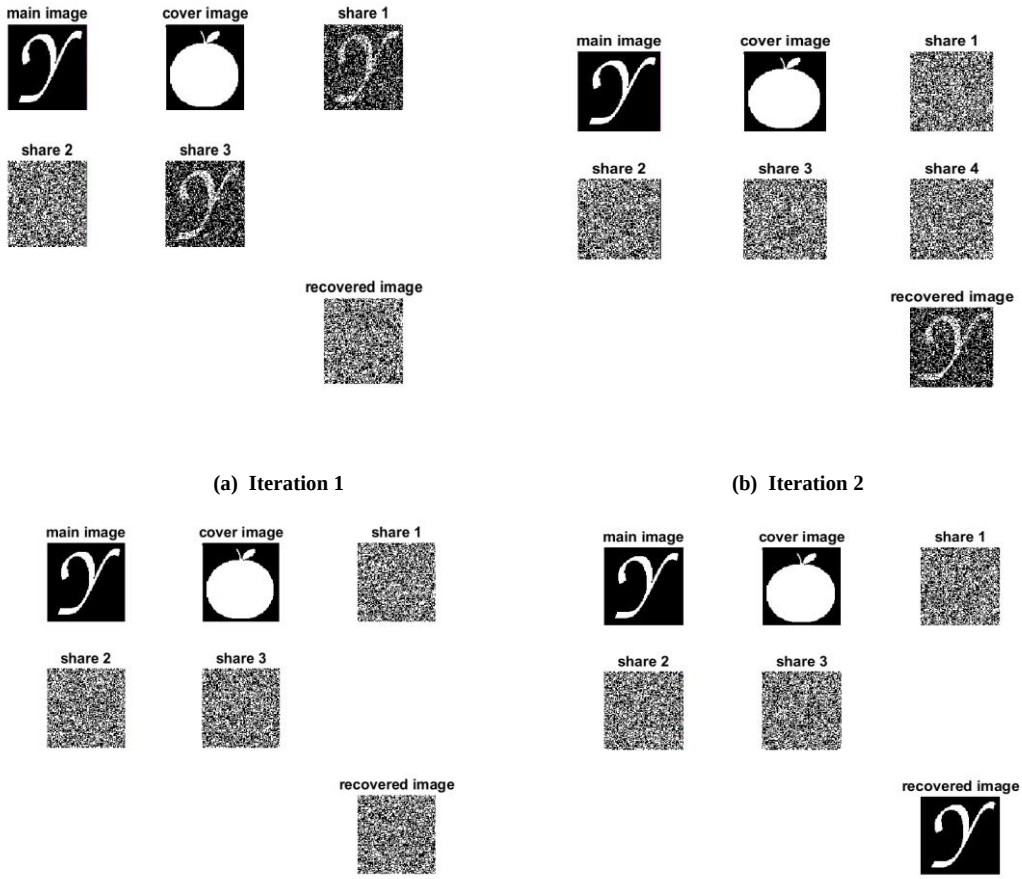
After generating noise-like shares by GA, we proceed to the construction of meaningful shares. To generate meaningful shares, we use another property of the XOR operation. According to the 1st property in Table 1, XOR can be written as follows:

$$r_1 \oplus C = r_1' \& C \otimes r_1 \& C'$$

If we call the obtained meaningless shares r_1 and the cover image C, then the meaningful shares R_{11} and R_{12} can be generated as follows:

$$R_{11} = r_1' \& C \qquad R_{12} = r_1 \& C'$$

For each noise-like share r_1, two meaningful shares R_{11} and R_{12} are constructed and given to one of the participants. These steps are shown in algorithm 7. For each of the meaningless shares, algorithm 7 is executed and meaningful share images are constructed.



(a) Iteration 1 **(b) Iteration 2**

(c) Iteration 3 **(d) Iteration 4**

Figure 7. Output of GA for different generations.

Algorithm 7

Input: Meaningless shares $\boldsymbol{r_1}.\boldsymbol{r_2}.\ldots.\boldsymbol{r_n}$, cover image C, numbers of shares n

Output: Meaningful share $\boldsymbol{R_{11}^i}$ and $\boldsymbol{R_{12}^i}$, $1 \leq \boldsymbol{i} \leq \boldsymbol{n}$

for each share i, $1 \leqslant$ i $\leqslant$ n do

construct $\boldsymbol{R_{11}^i}$ and $\boldsymbol{R_{12}^i}$ as follows:

$\boldsymbol{R_{11}^i} = \boldsymbol{r_1'} \& \boldsymbol{C}$

$\boldsymbol{R_{12}^i} = \boldsymbol{r_1} \& \boldsymbol{C'}$

end for

For more clarity, the diagram of step 1 for constructing meaningless shares is shown in Figure 8.

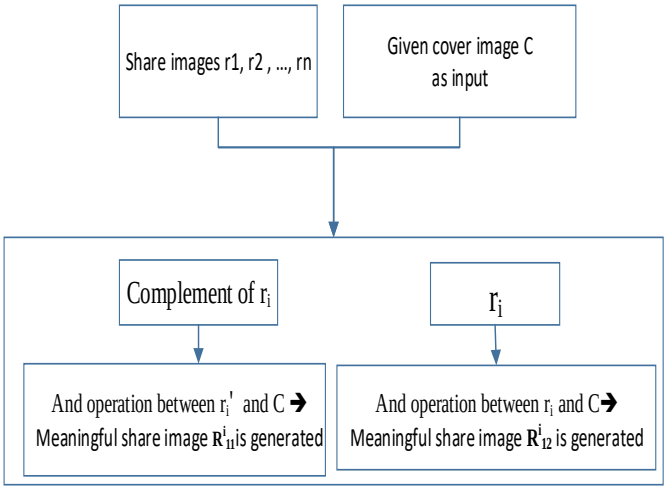


Figure 8. Diagram of constructing meaningless shares.

3.3. Recover secret image

In the image recovery phase, OR and XOR are used. First, two meaningful shares are stacked together by OR, and noise-like images R_i are produced. In the next step, these noise-like images are XOR-ed together to recover the input secret

image. These steps are clearly described in algorithm 8.

Algorithm 8

Input: Meaningless shares, cover image C, numbers of shares n

Output: Recovered secret image

If n is even do:

For n shares compute $\boldsymbol{R_i = R_{11}^i \otimes R_{12}^i . 1 \le i \le n}$ to reconstruct noise-like shares

($\otimes$ ***is for OR operation***)

The recovered secret image Rs is computed as:

$\boldsymbol{R_s = R_1 \oplus R_2 \oplus ... \oplus R_n}$(⊕ ***is XOR operation***)

End If

If n is odd do:

For n shares compute $\boldsymbol{R_i = R_{11}^i \otimes R_{12}^i . 1 \le i \le n}$ to reconstruct noise-like shares.

The recovered secret image Rs is computed as

$\boldsymbol{R_s = R_1 \oplus R_2 \oplus ... \oplus R_n \oplus C}$

End If

It should be noted that when n is even the output is as follows:

$$R_i = R_{11}^i \otimes R_{12}^i \ . 1 \le i \le n$$

$$R_i = r_i' \& C \otimes \ r_i \& C' = r_i \oplus C$$

$$R_s = R_1 \oplus R_2 \oplus ... \oplus R_n$$

$$= (r_1 \oplus C) \oplus \ (r_2 \oplus C) \oplus ... \oplus \ (r_n \oplus C)$$

$$= (r_1 \oplus r_2 \oplus ... \oplus r_n) \oplus \ (C \oplus C \oplus ... \oplus C)$$

$$= (r_1 \oplus r_2 \oplus ... \oplus r_n) \oplus 0$$

$$= (r_1 \oplus r_2 \oplus ... \oplus r_n)$$

when n is odd the output is as follows:

$$R_i = R_{11}^i \otimes R_{12}^i \ . 1 \le i \le n$$

$$R_i = r_i' \& C \otimes \ r_i \& C' = r_i \oplus C$$

$$R_s = R_1 \oplus R_2 \oplus ... \oplus R_n$$

$$= (r_1 \oplus C) \oplus \ (r_2 \oplus C) \oplus ... \oplus \ (r_n \oplus C)$$

$$= (r_1 \oplus r_2 \oplus ... \oplus r_n) \oplus \ (C \oplus C \oplus ... \oplus C)$$

$$= (r_1 \oplus r_2 \oplus ... \oplus r_n) \oplus (0 \oplus C) \oplus C$$

$$= (r_1 \oplus r_2 \oplus ... \oplus r_n) \oplus (0)$$

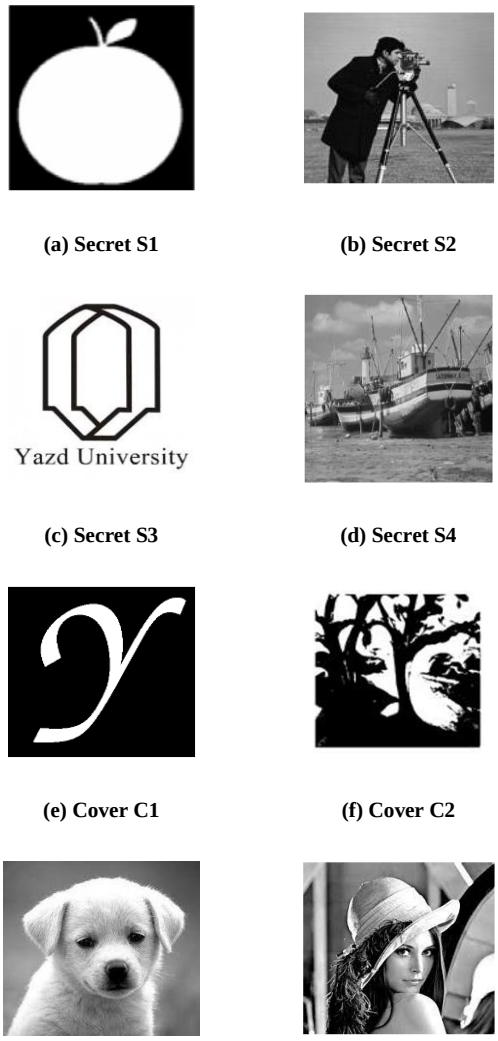
$$= (r_1 \oplus r_2 \oplus ... \oplus r_n)$$

4. Experimental Results and Analysis

This section indicates the experimental results to evaluate the performance of the proposed scheme. Simulation results are shown in Section 4-1. Comparison with other schemes and discussion are described in Section 4-2.

4.1.Simulation results

The images that are used to simulate and evaluate our scheme are shown in Figure 9. Figures a to d show images that are used as input secret image, and figures e to f are images that are used as cover images, respectively.



(a) Secret S1 **(b) Secret S2**

(c) Secret S3 **(d) Secret S4**

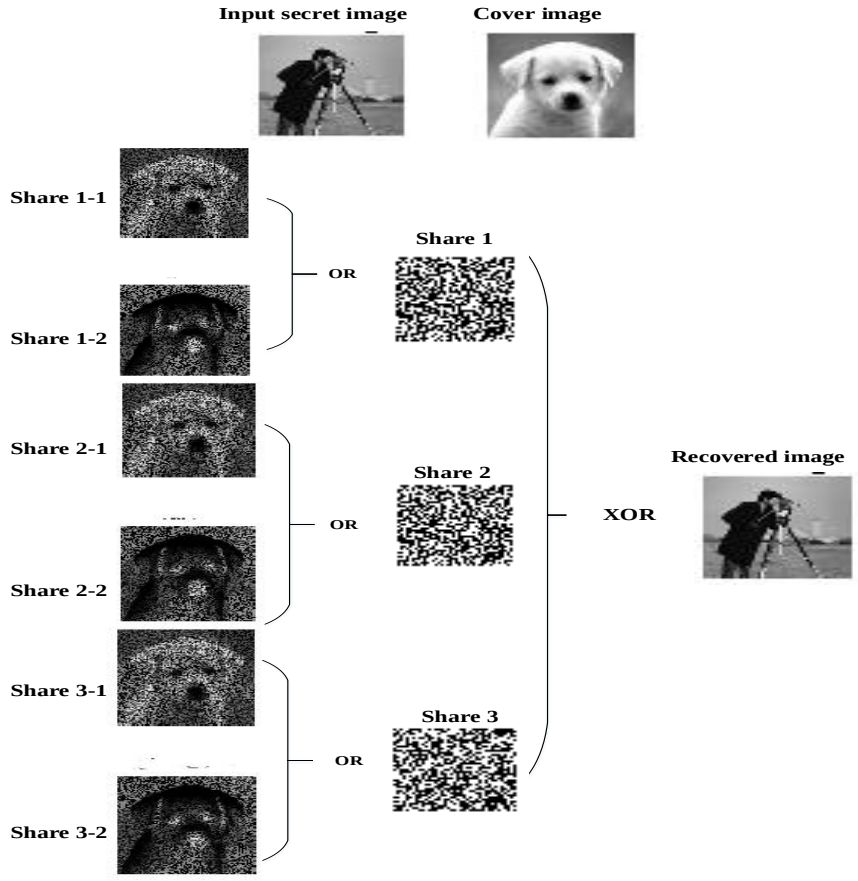
(e) Cover C1 **(f) Cover C2**

(g) Cover C3 **(h) Cover C4**

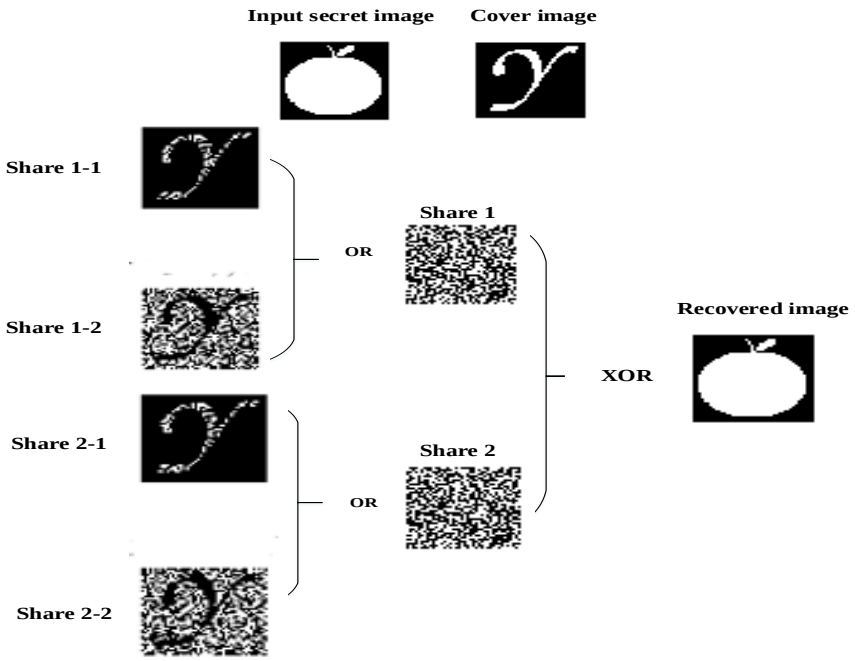
Figure 9. Secret and cover images used in our algorithm.

The simulation results of the proposed method are shown in Figure 10. These figures are shown for different n and input secret images. The first row is the input secret image and the cover image. In the 1st column, the meaningful shares are shown. The restored meaningless shares using OR are

shown in the 2nd column. The recovered secret image using XOR is shown in the 3rd column.



(a) Output for gray image with n = 3



(b) Output for binary image with n = 2

Figure 10. Output of proposed algorithm for different.

As you can see in Figure 10, the shares are meaningful. For each participant, two meaningful shares are created. For example, share 1-1 and share 1-2 is for participant 1, and so on. Finally, the recovered secret image is obtained by stacking all shared images of each participant using OR and then stacking all reconstructed images of the previous step using XOR.

4.2. Comparisons and discussions

Peak to Signal Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), Bit Correct Ratio (BCR), and Sensitivity and structural similarity index (SSIM) criteria have been used to evaluate the quality of the recovered image and shared images [25, 29, 30, 36].

• Mean Square Error (MSE)

This criterion calculates the sum of squares of the difference between two images f and g.

$$MSE = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[f(i,j)-g(i,j)]^2}{H \times W} \quad (8)$$

• Peak to Signal Noise Ratio (PSNR)

PSNR measures the similarity between two

images is PSNR.

$$PSNR = \log_{10}\frac{MAX^2}{MSE} \quad (9)$$

where MAX is the maximum possible pixel value in the image.

• Bit Error Rate (BER)

BER is calculation of the number of bit errors between two images f and g Where $\oplus$ is XOR operation.

$$BER = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} f(i,j) \oplus g(i,j)}{H \times W} \quad (10)$$

• Bit Correct Ratio (BCR)

BCR is sum of the number of same values between two images f and g.

$$BCR = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} \sim [f(i,j) \oplus g(i,j)]}{H \times W} \quad (11)$$

Where ~ stands for NOT operation.

- **Sensitivity and structural similarity index (SSIM)**

SSIM is a human vision system based measure where E(f) and E(g) are the average and S_f^2 and S_g^2 are the variances of images f and g. S_{fg} is covariance between f and g.

$$SSIM(f,g) = \frac{2 \times E(f) \times E(g) + C_1}{E(f)^2 + E(g)^2 + C_1} \times \frac{S_{fg} + C_2}{S_f^2 + S_g^2 + C_1} \quad (12)$$

The value of SSIM is between -1 and +1 where -1 means two image f and g are completely different and +1 means f and g are the same.

4.2.1. Evaluation of the recovered image

The results of the evaluation on different algorithms with different number of shares n are shown in tables 4 to 8, respectively. These values have been calculated between the recovered image and the input secret image.

Table 4. MSE of recovered image and input secret image.

Some schemes	Chiu [23]	Mohan [26]		Zhao [30]		Wang [29]		Our proposed
Secret/Cover	n ≥ 4	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n ≥ 2
S1/C1	0	0.2675	0.2431	0.2757	0.2564	0.1563	0.1223	0
S2/C2	0	0.4307	0.2484	0.4408	0.2629	0.1215	0.1225	0
S3/C3	0	0.2743	0.2769	0.2887	0.2943	0.1823	0.1423	0
S4/C4	0	0.2687	0.2495	0.2805	0.2608	0.1236	0.1567	0

Table 5. PSNR of recovered image and input secret image.

Some schemes	Chiu [23]	Mohan [26]		Zhao [30]		Wang [29]		Our proposed
Secret/Cover	n ≥ 4	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n ≥ 2
S1/C1	Inf	53.8583	54.2723	53.7266	54.0409	56.1912	57.2565	Inf
S2/C2	Inf	51.7889	54.1784	51.6884	53.9331	57.2850	57.2494	Inf
S3/C3	Inf	53.7485	53.7081	53.5268	53.4434	55.5229	56.5988	Inf
S4/C4	Inf	53.8386	54.1660	53.6510	53.9685	54.6361	56.1801	Inf

To determine the similarity between two images, MSE and PSNR should be low and high, respectively. In Table 4, MSE for the proposed method is zero and PSNR is Inf (Infinity). It indicates no difference between the input secret image and the recovered image.

Table 6. BER of recovered image and input secret image.

Some schemes	Chiu [23]	Mohan [26]		Zhao [30]		Wang [29]		Our proposed
Secret/Cover	n ≥ 4	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n ≥ 2
S1/C1	0	0.2675	0.2431	0.2757	0.2564	0.1563	0.1223	0
S2/C2	0	0.4307	0.2484	0.4408	0.2629	0.1215	0.1225	0
S3/C3	0	0.2743	0.2769	0.2887	0.2943	0.1823	0.1423	0
S4/C4	0	0.2687	0.2495	0.2805	0.2608	0.1236	0.1567	0

Table 7. BCR of recovered image and input secret image.

Some schemes	Chiu [23]	Mohan [26]		Zhao [30]		Wang [29]		Our proposed
Secret/Cover	n ≥ 4	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n ≥ 2
S1/C1	1	0.7325	0.7569	0.7243	0.7436	0.8437	0.8777	1
S2/C2	1	0.5593	0.7516	0.5592	0.7371	0.8785	0.8775	1
S3/C3	1	0.7257	0.7231	0.7113	0.7057	0.8177	0.8577	1
S4/C4	1	0.7313	0.7505	0.7195	0.7392	0.7764	0.8433	1

To determine the rate at which errors occur in a transmission system or not, we can use BER. In contrast BCR is used for correct bits in image. As you can see in Table 6 and Table 7, BER is zero and BCR is one for the proposed method.

Table 8. SSIM of recovered image and input secret image.

Some schemes	Chiu [23]	Mohan [26]		Zhao [30]		Wang [29]		Our proposed
Secret/Cover	n ≥ 4	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n ≥ 2
S1/C1	+1	0.2548	0.1256	0.2232	0.3232	0.8532	0.7432	+1
S2/C2	+1	0.4352	0.1546	0.3456	0.2785	0.8272	0.8478	+1
S3/C3	+1	0.2348	0.2348	0.2145	0.2465	0.8354	0.8522	+1
S4/C4	+1	0.2789	0.2479	0.1254	0.3447	0.8578	0.8421	+1

As you can see in our proposed method, the recovered secret image and the input secret image are the same. In chiu's method the SSIM is also +1 but the difference between this method and our is quality of share images.

4.2.2. Evaluation of share images

The results of the similarity between shares and cover image are shown in Tables 9 to 13.

The values in these tables indicate high-quality of share images in our proposed method. In the proposed method, in addition to similarity of the input secret image and recovered image, the high similarity between the shares and cover image is also achieved. The values in tables are average of the number of n shares.

Table 9. Average MSE of share images and cover image.

Some schemes	Chiu [23]		Mohan [26]		Zhao [30]		Wang [29]		Our proposed	
Secret/Cover	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5
S1/C1	0.2914	0.2852	0.2574	0.2460	0.4997	0.5092	0.1263	0.1123	0.0584	0.0580
S2/C2	0.2726	0.2686	0.2478	0.2728	0.5031	0.5013	0.1115	0.2484	0.2698	0.0925
S3/C3	0.2594	0.2610	0.2968	0.2983	0.5115	0.4981	0.1023	0.0823	0.2944	0.2528
S4/C4	0.2751	0.2753	0.2750	0.2592	0.5020	0.5023	0.1026	0.0867	0.2552	0.2539

Table 10. Average PSNR of share images and cover image.

Some schemes	Chiu [23]		Mohan [26]		Zhao [30]		Wang [29]		Our proposed	
Secret/Cover	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5
S1/C1	53.4856	53.5800	54.0243	54.2222	51.0619	51.0615	57.1168	57.6270	60.4667	60.4965
S2/C2	53.7752	53.8394	54.1902	53.7724	51.1143	51.1298	57.6581	54.1785	53.8200	58.9663
S3/C3	53.9915	53.9640	53.4062	53.3843	51.0423	51.1576	58.0320	58.9768	54.1537	54.1023
S4/C4	53.7364	53.7322	54.0266	54.1007	51.1238	51.1212	58.0193	58.7506	54.0620	54.0842

Average MSE and PSNR in Table 9 and Table 10 show the similarity between the shares and cover image. The number of shared images is more than one image; this value is calculated as an average. According to the tables and comparing the results, it can be seen that in the proposed method, the share image is very similar to the cover image. It can be concluded that the proposed method generates high quality meaningful shares.

Table 11. Average BER of share images and cover image.

Some schemes	Chiu [23]		Mohan [26]		Zhao [30]		Wang [29]		Our proposed	
Secret/Cover	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5	n = 4	n = 5
S1/C1	0.2914	0.2852	0.2574	0.2460	0.4997	0.5092	0.1263	0.1123	0.0584	0.0580
S2/C2	0.2726	0.2686	0.2478	0.2728	0.5031	0.5013	0.1115	0.1484	0.2698	0.0925
S3/C3	0.2594	0.2610	0.2968	0.2983	0.5115	0.4981	0.1023	0.0823	0.2944	0.2528
S4/C4	0.2751	0.2753	0.2750	0.2592	0.5020	0.5023	0.1026	0.0867	0.2552	0.2539

Table 12. Average BCR of share images and cover image.

Some schemes	Chiu [23]		Mohan [26]		Zhao [30]		Wang [29]		Our proposed	
Secret/Cover	**n = 4**	**n = 5**	**n = 4**	**n = 5**	**n = 4**	**n = 5**	**n = 4**	**n = 5**	**n = 4**	**n = 5**
S1/C1	0.7086	0.7148	0.7426	0.7540	0.5003	0.4908	0.8737	0.8877	0.9416	0.9420
S2/C2	0.7274	0.7314	0.7522	0.7272	0.4969	0.4987	0.8885	0. 8516	0.7302	0.9075
S3/C3	0.7406	0.7390	0.7032	0.7017	0.4885	0.5019	0.8977	0.9177	0.7501	0.7472
S4/C4	0.7249	0.7247	0.7427	0.7471	0.4980	0.4977	0.8974	0.9133	0.7448	0.7461

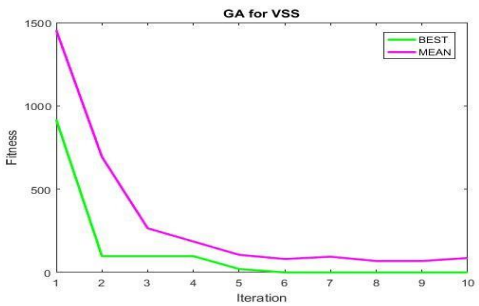
In Table 11 and Table 12, the value of BER and BCR is shown for different number of shares. These criteria of our scheme are better than other methods. It indicates low difference between the shared image and the cover image. Recovered images of scheme by Zhao and our proposed are lossless. The difference between these schemes is quality of shares.

The quality of shares in our proposed method is higher. Also Zhao's method has a limit on number of shares that is it works for $n \geq 4$. If the number of shares is less than 4, the method is not lossless anymore.

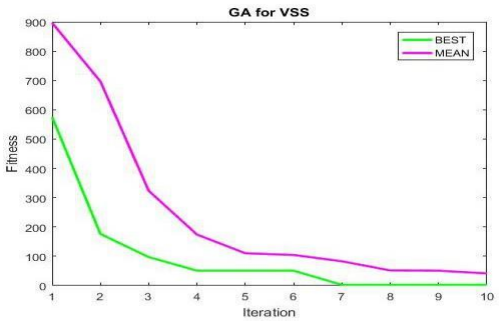
Table 13. Average SSIM of share images and cover image.

Some schemes	Chiu [23]		Mohan [26]		Zhao [30]		Wang [29]		Our proposed	
Secret/Cover	**n = 4**	**n = 5**	**n = 4**	**n = 5**	**n = 4**	**n = 5**	**n = 4**	**n = 5**	**n = 4**	**n = 5**
S1/C1	0.3523	0.4615	0.1523	0.1789	-0.5635	-0.8851	0.7252	0.7125	0.8723	0.8915
S2/C2	0.3625	0.4212	0.1215	0.4212	-0.8325	-0.7523	0.7215	0.6545	0.8625	0.8845
S3/C3	0.3215	0.3998	0.0112	0.3915	-0.8712	-0.9231	0.7412	0.5623	0.8459	0.8814
S4/C4	0.3874	0.4016	0.0169	0.3516	-0.8512	-0.9125	0.7325	0.5684	0.8948	0.9210

The convergence diagram of GA is shown in Figure 11. The diagram is displayed in two modes, the mean and the best candidate. The horizontal axis is the number of iterations and the vertical axis is the cost function. As it can be seen, the algorithm has converged in low iterations.



(a) Convergence of figure 7.a



(b) Convergence of figure 7.b

Figure 11. Convergence diagram of GA in proposed method.

Some features of visual secret sharing in previous works are summarized in Table 12. In the 1st column, type of input secret images is specified. The 2nd feature checks the pixel expansion. The 3rd column is the meaningfulness of the share images or not. In the 4th column, it is specified how to restore the image with OR or XOR. The

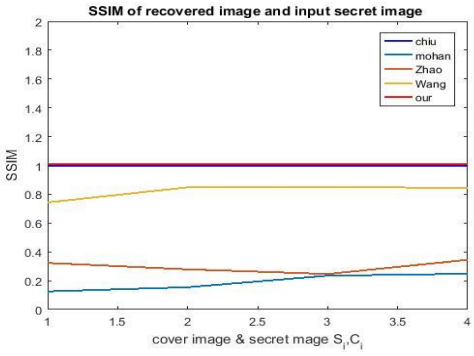
last column shows the quality of the restored image.

Table 14. Comparison of visual secret sharing features.

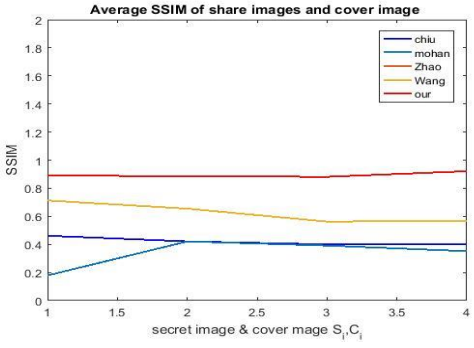
Schemes	Type of image	Pixel expansion	Meaningful shares	Recover mode	Contrast
Shyu [20]	Binary/Halftone	Yes	No	XOR	Low
Kukreia [32]	Binary/Halftone	No	No	XOR	High
Ou [25]	Binary/Halftone	No	Yes	XOR	High
Zhao [30]	Binary/Gray	No	No	OR	High
Mohan [26]	Binary/Halftone	Yes	Yes	XOR	High
Chiu [23]	Binary/Halftone	No	Yes	XOR	$\alpha = 1$
Wang [29]	Binary/Halftone	No	Yes	XOR	High
Our scheme	Binary/Gray	No	Yes	OR/ XOR	$\alpha = 1$

4.2.3 Visual quality of shared images and recovered image

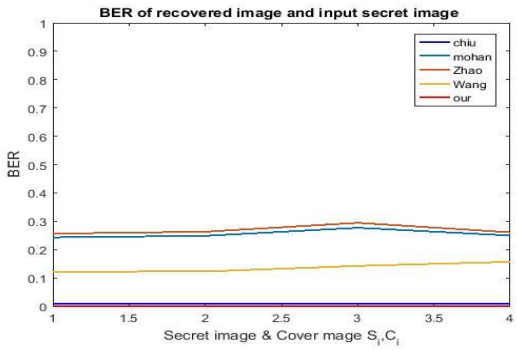
In order to check the quality of recovered secret image and shared images in our proposed method with other methods, the PSNR and SSIM diagram for different number of shares is shown in Figure 12.



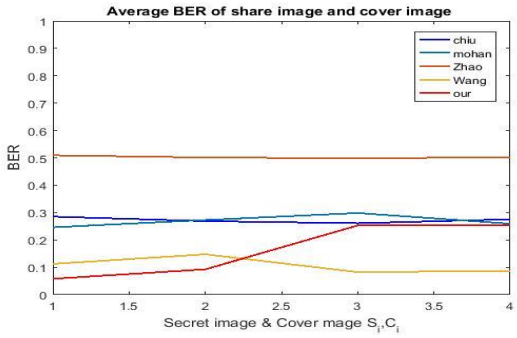
(a) SSIM of recovered image and input secret image



(b) SSIM of shared images and cover image.



(c) BER of recovered image and input secret image



(d) BER of shared images and cover image

Figure 12. Visual quality of shared images and recovered image.

5. Conclusion

In this research, a lossless meaningful visual secret sharing using properties of XOR has been introduced. First, the proposed method searches suitable matrices M_0 and M_1 by GA. Next, with these matrices, noise-like shares are generated. By stacking share images, the input secret image is fully recovered. According to other properties of XOR, the noise-like shares become meaningful

shares. The evaluations show that the proposed method has an acceptable performance in quality of recovered and shared images. Evaluation is performed with PSNR, MSE, BER and BCR criteria. To the best of our knowledge, these criteria are acceptable for a novel meaningful visual secret sharing.

References

[1] H. Khodadadi and A. Zandvakili, "A New Method for Encryption of Color Images based on Combination of Chaotic Systems," *Journal of AI and Data Mining*, vol. 7, pp. 377–383, 2019.

[2] R. Sangeetha, G. Koteeswari, and M. Phil, "Securing Data in IOT using Cryptography and Steganography Techniques," *Int. J. Res. Eng. Sci.*, vol.9, pp. 1–5, 2021.

[3] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, pp. 612–613, 1979.

[4] J.C. Ku-Cauich and G. Morales-Luna, "A linear code based on resilient Boolean maps whose dual is a platform for a robust secret sharing scheme," *Linear Algebra and its Applications*, vol. 596, pp. 216-229, 2020.

[5] C.C Thien and J.C Lin., "Secret image sharing," *Computer and Graphics*, vol. 26, pp. 765–770, 2020.

[6] R.Z. Wang and C.H Su, "Secret image sharing with smaller shadow images," *Pattern Recognition Letters*, vol. 27, pp. 551–5, 2006.

[7] X. Jia, Y. Guo, X. Luo, D. Wang, and C. Zhang, "perfect secret sharing scheme for general access structures," *Information Sciences*, vol. 595, pp. 54-69, 2022.

[8] S. Charoghchi and S. Mashhadi, "Three (t, n)-secret image sharing schemes based on homogeneous linear recursion," Information *Sciences*, vol. 552, pp. 220-243, 2021.

[9] C.C Yang, T.Y Chang, M.S Hwang. A (t, n) multi-secret sharing scheme, "Applied *Mathematics and Computation*," vol.151, pp.483-490, 2004.

[10] M. Naor and A. Shamir, "Visual cryptography," *Workshop on the theory and application of cryptographic techniques*, pp. 1–12, 1994.

[11] P. Singh, B. Raman, and M. Misra, "A (n, n) threshold non-expansible XOR based visual cryptography with unique meaningful shares," *Signal Processing*, vol. 142, pp. 301–319, 2018.

[12] M. Gupta and D. Chauhan, "A visual cryptographic scheme to secure image shares using digital watermarking," *International Journal of Computer Science and Information Technologies***,** vol. 6, pp. 4339–4343.

[13] C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," *Computers & Graphics*, vol. 22, pp. 449-455, 1979.

[14] P.L. Chiu and K.H Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 992–1001, 2011.

[15] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Optics letters*, vol. 12, pp. 377–379,1987.

[16] T.H Chen and K.H Tsao, "Visual secret sharing by random grids revisited," *Pattern recognition*, vol. 42, pp. 2203–2217, 2009.

[17] X. Yan, X. Liu, and C.N Yang, "An enhanced threshold visual secret sharing based on random grids," *Journal of real-time image processing*, vol. 14, pp. 61-73, 2018.

[18] H.C Chao and T.Y Fan, "XOR-based progressive visual secret sharing using generalized random grids," *Displays*, vol. 49, pp. 6-15, 2017.

[19] S.J Shyu, "Image Encryption by Random Grids," *Pattern Recognition*, vol. 40, pp.1014-031, 2007.

[20] R.G. Sharma, P. Dimri, and H. Garg, "Visual cryptographic techniques for secret image sharing: a review," *Information Security Journal: A Global Perspectiv*, vol. 27, pp. 241–259, 2018.

[21] C.C. Chang, Y.H. Chen, and H.C. Wang, "Meaningful secret sharing technique with authentication and remedy abilities," *Information Sciences*, vol.181, pp. 3073-3084, 2011.

[22] P.L Chiu and K.H Lee. "Efficient constructions for progressive visual cryptography with meaningful shares," *Signal Processing*, vol. 165, pp. 233–249, 2019.

[23] D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operation," *Pattern Recognition*, vol. 40, pp. 2776–2785, 2007.

[24] D. Ou, W. Sun, and X. Wu, "Non-expansible XOR-based visual cryptography scheme with meaningful shares," *Signal Processing*, vol. 108, pp. 604–621, 2015.

[25] J. Mohan and R. Rajesh, "Secure visual cryptography scheme with meaningful shares," *Indian Journal of Computer Science and Engineering*, Vol. 11, pp.146–160, 2020.

[26] Z. Wang, R.G. Arce, and G. Di Crescenzo. "Halftone visual cryptography via error diffusion," *IEEE transactions on information forensics and security*, vol. 4, pp. 383–396, 2009.

[27] M.E. Hodeish and V.T. Humbe, "An optimized halftone visual cryptography scheme using error diffusion," *Multimedia Tools and Applications*, vol. 19, pp. 24937–24953, 2018.

[28] S. Wang, Y. Lu, X. Yan, L. Li, and Y. Yu, "AMBTC-based visual secret sharing with different meaningful shadows," *Mathematical Biosciences and Engineering*, vol. 18, pp. 5236-5251, 2021.

[29] Y. Zhao and F.W. Fu, "A cheating immune (k, n) visual cryptography scheme by using the rotation of shares," *Multimedia Tools and Application***,** vol. 81, pp. 6235-6257, 2002.

[30] P.A. Eisen and D.R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, Designs," *Codes and Cryptography*, vol. 25, pp. 15–61, 2002.

[31] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual cryptography for general access structures*," Information Computation,* vol. 129, pp. 86–106,1996.

[32] S. Kukreja, G. Kasana, and S.S Kasana. "Cellular automata based image authentication scheme using extended visual cryptography," *Computing and Informatics*, vol. 38, pp.1272–1300, 2019.

[33] L. Chandana Priya, K, "Praveen. (t, k, n). Deterministic extended visual secret sharing scheme using combined Boolean operations," *International Conference on Information Processing*, vol. 22, pp. 66-77, 2021.

[34] S. Shivani, "Multi-secret sharing with unexpanded meaningful shares," *Multimedia Tools and Applications*, vol. 77, pp. 6287–6310, 2018.

[35] S.P Kannojia and J. Kumar, "XOR-based visual secret sharing scheme using pixel vectorization," *Multimedia Tools and Applications*, vol. 80, pp. 14609–14635, 2021.

[36] L. Liu, Y. Lu, and X. Yan. "A novel (k1, k2, n)-threshold two-in-one secret image sharing scheme for multiple secrets," *Journal of Visual Communication and Image Representation*, vol. 1, pp. 102971, 2021.

[37] C.N. Yang and D.S. Wang, "Property analysis of XOR-based visual cryptography," *IEEE transactions on circuits and systems for video technology*, vol. 24(2), pp. 189-197, 2013.

[38] A. Nag, J.P. Singh, and A.K Singh, "An efficient Boolean based multi-secret image sharing scheme," *Multimedia tools and applications*, vol. 79, pp. 16219-16243, 2020.

[39] K. Bhat, U.K. Reddy KR, R. Kumar HS, and D. Mahto, "A novel scheme for lossless authenticated multiple secret images sharing using polynomials and extended visual cryptography," *IET Information Security*, vol. 15, pp. 13-22, 2021.

[40] S.S Lee, J.C. Na, S.W. Sohn, C. Park, D.H. Seo, and S.J. Ki, "Visual cryptography based on an interferometric encryption technique," ETRI *journal*, Vol. 24, pp. 373-380, 2002.

[41] S. Kumar and R.K. Sharma, "Threshold visual secret sharing based on Boolean operations," *Security and Communication Networks*, vol. 7, pp. 653-664, 2014.

[42] T.Y. Fan and H.C. Chao, "User-friendly XOR-based visual secret sharing by random grid," *IET Information Security*, vol. 12, pp. 398-403, 2018.

[43] D. Taghaddos and A. Latif, "Visual cryptography for gray-scale images using bit-level*," Journal of Information Hiding and Multimedia Signal Processing*, vol. 5(1), pp. 90-97, 2014.

[44] P.D. Shah and R.S Bichkar, "Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure," *Engineering Science and Technology*, vol. 24, pp. 782-794, 2021.

روشی جدید برای تسهیم راز بصری معنادار با بازیابی کامل توسط ویژگی‌های های عملگر XOR

زینب مهرنهاد[۱]، علی‌محمد لطیف[۱،*] و جمال زارع‌پور احمدآبادی[۲]

[۱] **دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران.**

[۲]**دانشکده علوم کامپیوتر، دانشگاه یزد، یزد، ایران.**

ارسال ۲۰۲۲/۱۲/۱۹؛ بازنگری ۲۰۲۳/۰۱/۳۱؛ پذیرش ۲۰۲۳/۰۳/۰۷

چکیده:

در این پژوهش، یک طرح جدید برای تسهیم راز بصری معنا دار با بازیابی کامل تصویر رمز با استفاده از ویژگی های XOR ارائه شده است. در مرحله اول، الگوریتم ژنتیک با تابع هدف پیشنهادی مناسب، تصاویر سهم نویزی ایجاد می‌کند. این تصاویر هیچ اطلاعاتی در مورد تصویر رمز اصلی ندارند و با چیدن آن‌ها در کنار هم، تصویر رمز اصلی به طور کامل بازیابی می شود. به دلیل حملاتی که هنگام انتقال تصویررخ می‌دهد، رویکرد جدیدی برای ساخت سهم‌های معنادار توسط ویژگی‌های XOR پیشنهاد شده است. در مرحله بازیابی، تصویر رمز اصلی به طور کامل توسط عملگر XOR بازیابی می شود. روش پیشنهادی با استفاده از معیارهای PSNR، MSE و BCR ارزیابی می‌شود. آزمایش‌ها نتایج خوبی را در مقایسه با روش‌های دیگر از نظرکیفیت تصاویر سهم و کیفیت تصویر بازیابی شده ارائه می‌دهند.

کلمات کلیدی: تسهیم راز معنا دار، تسهیم راز، تسهیم راز بصری، الگوریتم ژنتیک.