DOI: 10.2478/ias-2025-0005 • JIAS • 20(2) • 2025 • 74-85

(*n*, *n*) Multi-Secret Image Sharing Scheme with Enhanced Quality Meaningful Shares

Yogesh K. Meghrajani[1*], Vishakha J. Kapadiya[1] and Laxmi S. Desai[2]

1 Department of Electronics & Communication, Dharmsinh Desai University, Nadiad 387001, India; vishakhakapadiya44@gmail.com

2 Department of Mathematics, Dharmsinh Desai University, Nadiad 387001, India; laxmidesai.ec@ddu.ac.in

*Correspondence author: yogesh_engg2.ec@ddu.ac.in

Abstract: Traditional visual secret sharing (VSS) schemes that encrypt secret images into noise-like images have been extended to multiple secret sharing (MSS) schemes to share multiple secret images using meaningful shares. Due to poor visual quality, such schemes are vulnerable to attacks from intruders. In this paper, we propose an efficient (n, n) MSS scheme for sharing n secret images, where n cover images are embedded in n meaningful shares. The proposed scheme provides improved visual quality with higher sharing capacity. Security is enhanced by meaningful share images. Thus, the proposed scheme offers enhanced quality and efficiency while satisfying security criteria.

Keywords: Meaningful visual secret sharing scheme (n, n) multi-secret image sharing, XOR-based visual secret sharing, visual quality of meaningful shares, image hiding scheme.

1 Introduction

In today's digital era, security of shared images is more prevalent. Visual secret sharing (VSS) or secret image sharing (SIS) schemes offer the security of the shared images from theft, modification, and destruction compared to raw images. VSS schemes encrypt the secret image before sharing, using cryptographic techniques. In traditional VSS schemes, the poor contrast of recovered image is inevitable due to its stacking property. Thus, Boolean-based secret sharing schemes have received widespread accolades by adding little computation to improve the quality of recovered images. Additionally, the use of multi secret sharing (MSS) schemes increases the sharing capacity of VSS schemes. Several researchers [1],[2],[3],[4],[5],[6] have proposed Boolean-based MSS schemes for sharing multiple secrets using meaningless shares. Chen and Wu [1] presented a Boolean-based MSS scheme but their scheme has a sharing capacity of (n, n + 1). Moreover, [2] identified the security shortcoming in the Chen and Wu [1] method. Hence, they proposed an MSS scheme to overcome this drawback besides improvement in the sharing capacity to (n, n). Yang et al. [3] reported a compromised threshold security of [2] and introduced MSS scheme using SHA-160 and torus automorphism. Furthermore, Chen et al. [4] enhanced the security of the MSS scheme using SHA-256. In [5], Nag et al. proposed multi-secret sharing scheme for a (t, n) general access structure (GAS) scheme, in which any t shares from n shares can recover secret images. A multilevel MSS was introduced by Bisht and Deshmukh [7], with higher levels representing an increased number of shares. Rawat et al. [8] proposed an MSS scheme designed to handle secret images of varying dimensions. Furthermore, the MSS scheme [9] utilized DNA encryption techniques enables the verification of cheating attempts. Besides these schemes, related research reported for watermarking technique [10], mathematical modeling [11], and a model-driven approach for information security [12].

In the aforementioned schemes, the third party can evidently suspect the presence of a secret because of the meaningless share images. Thus, to overcome this problem, a meaningful VSS scheme is adopted to share a secret image. An RG-based meaningful VSS scheme was proposed by Hou et al. [13]. Further, Boolean-based meaningful VSS schemes were proposed by [14], An authenticatable (2, 3) secret sharing scheme was proposed by [15], and [16] presented an essential secret image sharing approach. Other meaningful VSS schemes are based on general meaningful shadow construction [17] and turtle shell structure matrix [18]. Additionally, Kapadiya et al. [19] showed a Boolean-based VSS technique to generate meaningful shares by embedding a different number of bits of secret image. Their study showed that embedding four bits of secret image into meaningful shares offers optimal results.

The aforementioned meaningful VSS schemes are extended for sharing multiple secret images. Refs. [20], [21], [22], [23] proposed Boolean-based meaningful MSS schemes and [24] proposed RG-based meaningful MSS scheme. Reddy and Prasad [20] generated meaningful shares by using Boolean-based operations. Though their scheme achieved lossless recovery of secret images, the number of meaningful shares is three times the number of secrets. Shivani et al. [21] proposed XOR-based meaningful MSS scheme for store-and-forward telemedicine applications. Their scheme encrypts n secrets using n cover images and a secret key to generate n meaningful shares. The secret key is utilized during encoding and decoding to generate an additional or master share. The secret key is required to transmit along with *n* shares. Therefore, their scheme effectively offers sharing capacity as (*n, n* + 1). Moreover, although their scheme provides a high quality reconstructed image, the quality of meaningful shares is poor. Ref. [22] proposed a meaningful MSS scheme using a universal share. This scheme encodes n secret images into a meaningful universal share and n meaningful shares. This scheme also requires n+1 shares including the universal share, for sharing n secrets.

To the best of our knowledge, an (*n, n*) MSS scheme that generates meaningful shares and offers high-quality recovered secret images as well as meaningful shares has not been proposed so far. In this paper, we propose an efficient (*n, n*) MSS scheme using meaningful shares. The proposed scheme generates n meaningful shares using n cover images for n secret images. Meaningful shares are generated by employing Boolean XOR, torus automorphism, SHA-256 and bit shift functions on input images. Notable contributions of this manuscript are: (I) the proposed scheme has high efficiency as it needs only n shares for sharing n secrets, (II) this scheme generates meaningful shares to reduce suspicion, (III) the proposed scheme achieves improved quality of share and recovered images, (IV) the proposed scheme supports both gray and color secret image formats. Hence, the proposed scheme reduces the number of meaningful shares while improving the quality of both meaningful shares and recovered secret images.

The rest of this paper is organized as follows: Section II presents the proposed scheme. Section III describes experimental results and analysis. Section IV explains comparison and discussion. Lastly, we conclude this study in Section V.

2 Proposed Scheme

This section explains an efficient (*n, n*) MSS scheme with meaningful shares. The sharing process involves generation of random shares to enhance the security of the shared images. The proposed scheme utilizes these random shares along with cover images to generate meaningful shares. In the recovery process, random shares are generated using meaningful shares to decrypt the secret images. Hence, random shares are not required to transmit with meaningful shares in the proposed scheme. Therefore, the proposed scheme qualifies as an (*n, n*) MSS scheme. The proposed scheme is described for grayscale secret images. In the same manner, it is acceptable for color images. Experimental results are presented for both grayscale and color images.

2.1 Sharing Procedure

This section describes the process of random share generation, followed by meaningful share generation. During encryption, secret images G_k (k = 1, 2, ...,n), cover images C_k (k = 1, 2, ...,n), and intermediate random images R_k (k = 1, 2, ..., n/2) generate n meaningful share images S_k (k = 1, 2, ..., n). The dimensions of these images are $M * M$.

2.1.1. *Random Share Generation in Sharing Process*

In the random share generation process, cover images are considered as input images to generate random shares of size $M * M$. Secret image is embedded in another image which is called a cover image. Cover image embeds a secret image and serves as a meaningful share. These random shares are employed to enhance the security of the secret images. The high-nibble segment of the cover images utilized to generate random shares are part of meaningful shares too. Hence, random shares do not need to be transmitted separately. The random share generation procedure is illustrated below.

Step 1:

$$h \leftarrow SH\ A256\left(C_1\left(5-8\right) \oplus C_2\left(5-8\right) \oplus \cdots \oplus C_n\left(5-8\right)\right) \tag{1}$$

$$h_1\left(x, y\right) \leftarrow \text{Circular padding}(h) \tag{2}$$

Where, $C_k(5-8)$ = higher nibble of cover image k.

Eq. (1) applies a bitwise XOR operation to the higher nibble of all cover images. The share images contain these higher nibble, which are used to randomize the content of the secret image. The result of the bitwise XOR operation is passed as input to the SHA-256 algorithm, which converts it into $1 * 64$ hexadecimal hash value. Next, h_1 is generated with the same size as the input image by applying circular rotation of h and padding into h_1. The circular rotation of h further randomizes the content of the secret image.

Step 2:

Although h is highly secure, there is a concern about randomness of the padded image h_1, since it is generated by a circular rotation of h. To enhance randomness, we randomly permute the pixels of the image. The modified image is a chaotic rearrangement of pixels without affecting their intensity values. To permute h_1, the widely known Torus automorphism approach [3] is employed. h_1 of size $M * M$ with 256 greyscales has pixel value $h_1(x, y) \epsilon (0,255)$, where $0 \le x, y \le M-1$. Torus automorphism is defined in Eq. (3) [3] as,

$R_0'(x', y')$= Torus automorphism $(h_1(x, y))$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} x+y \\ h_1(x,y) * x + h_1(x,y) * y + y \end{bmatrix} mod(M) \tag{3}$$

Where, x' and y' represent new pixel coordinates of the modified random image $R_0'(x', y')$ and M is the size of input image.

Step 3:

Using a single random image for all secret images poses a security threat to the scheme. Therefore, different random images are generated using the base random image. Moreover, since only a nibble of a random image is required in the encoding phase, one random image is used in two meaningful shares.

$$R_k'(x', y') \leftarrow \text{bitshift}\left(R_0'(x', y'), (x' + y' + k) mod\ 8\right) \tag{4}$$

$$R_k = \begin{cases} R'_{(k+1)/2}(5-8), & \text{if } (k\%2) \neq 0 \\ R'_{(k)/2}(1-4), & \text{if } (k\%2) = 0 \end{cases} \tag{5}$$

Where, $k = 1, 2, ..., n/2$, the bitshift function applies a circular left shift by shift value $[(x + y + k)\ mod 8]$ bits to each pixel $R_0'(x', y')$.

2.1.2. *Generation of Meaningful Shares*

Meaningful shares are generated by embedding the nibble of cover and secret images. The security of secret images is ensured by incorporating random shares, while their appearance is maintained by inserting the high nibble of cover images into the high nibble of meaningful shares. In the proposed scheme, the following steps are included in the encoding phase.

$$\begin{aligned} S_k(1-4) &\leftarrow G_k(5-8) \oplus C_k(5-8) \oplus R_k \\ S_k(5-8) &\leftarrow C_k(5-8) \end{aligned} \tag{6}$$

Here, $S_k(1-4)$ = lower nibble of meaningful share image k, $G_k(5-8)$ = higher nibble of secret image k, $S_k(5-8)$ = higher nibble of meaningful share image k, and $C_k(5-8)$ = higher nibble of cover image k.

For two secret images, S_1 and S_2 are computed as follows:,

$S_1(1-4) \leftarrow G_1(5-8) \oplus C_1(5-8) \oplus R_1(5-8), S_1(5-8) \leftarrow C_1(5-8).$

$S_2(1-4) \leftarrow G_2(5-8) \oplus C_2(5-8) \oplus R_1(1-4), S_2(5-8) \leftarrow C_2(5-8).$

For example, consider two secret images, two cover images, and a random share image, where pixel values are: $G_1 = 220$, $G_2 = 148$, $C_1 = 122$, $C_2 = 80$, and $R_1 = 10$, respectively. Using Eq. (6), we obtain: $S_1 = 123$ and $S_2 = 86$.

Theorem 1 Meaningful shares S_k ($k = 1, ..., n$) generated during the encryption process resemble the cover images C_k and achieve considerably high peak signal to noise ratio (PSNR) value.

Proof 1 During the encryption process, meaningful shares are generated by embedding the high nibble of cover images into the high nibble of meaningful shares. The high nibble contributes significantly to the overall image appearance, whereas low-order bits contribute to more subtle intensity details in the image. For an 8-bit grayscale image, each pixel has maximum value of 255. The maximum contribution of the high nibble is 240, while the maximum contribution of the low nibble is 15. Since high nibble of meaningful share images is identical to the high nibble of their corresponding cover images, the worst-case difference between cover image pixels and meaningful share pixels is 15. This ensures a high degree of similarity of meaningful shares and cover images.

To quantify the similarity, Peak signal to noise ratio (PSNR) is calculated. PSNR [25] is defined as,

$$PSNR = 20 * log_{10}\left(\frac{255}{\sqrt{MSE}}\right) dB \tag{7}$$

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I(i,j) - I'(i,j)\right)^2$$

I (i, j) indicates intensity of the cover image and I'(i, j) represents intensity of the meaningful share image.

PSNR is a renowned numerical parameter to measure the visual quality of a given image. A higher PSNR value indicates better match between the images under observation. A PSNR value above 30 dB signifies high-quality images [26], which in our case, refers to meaningful shares. The worst-case PSNR is 24.61 dB, assuming all low-nibble pixel values of I (i, j) and I' (i, j) are different. However, in the average-case scenario, the PSNR is 30.63 dB. Empirically, we calculated the PSNR value 1000 times and observed the values above 30 dB, demonstrating the high quality of meaningful shares.

2.2 Algorithm for Meaningful Share Generation

The encryption algorithm describes the procedure to generate n meaningful shares from n secret and n cover images. The following is the Algorithm 1 for meaningful share generation.

Algorithm 1: Algorithm for meaningful share generation

Input: n secret images (G_k) and n cover images (C_k) of size $M \times M$
Output: n meaningful share images (S_k) of size $M \times M$
Define: m is a bit number, $S_k^{(m)}(i,j)$ = lower nibble of meaningful share image k at (i, j) $G_k^{(m+4)}(i,j)$ = higher nibble of secret image k at (i, j) $S_k^{(m+4)}(i,j)$ = higher nibble of meaningful share image k at (i, j)

1: for $n \leftarrow 1$ to k do
2: for $i \leftarrow 1$ to M do
3: for $j \leftarrow 1$ to M do
// Generate intermediate random shares R_k
4: Follow the Eq. (1) to generate h
5: Generate shares R_k using h and Eq. (2) to Eq. (5)
// Generate meaningful shares
6: for $m \leftarrow 1$ to 4
7: $S_k^{(m)}(i,j) \leftarrow G_k^{(m+4)}(i,j) \oplus C_k^{(m+4)}(i,j) \oplus R_k$
8: $S_k^{(m+4)}(i,j) \leftarrow C_k^{(m+4)}(i,j)$
9: end for
10: end for
11: end for
12: end for
13: return S_k

2.3 Recovery Procedure

The secret image decryption process is explained in this section.

2.3.1. *Random Share Generation in Recovery process*

Sheer meaningful shares are required to generate random shares in the recovery phase. Thus, meaningful shares of size $M * M$ are considered as input images in the process. During encryption, the high nibble of cover images are utilized to generate random shares, which are subsequently embedded in the high nibble of meaningful shares. High nibble of meaningful shares are used to generate the hash function h' as shown below.

$$h' \leftarrow SH\ A256\left(S_1(5-8) \oplus S_2(5-8) \oplus \cdots \oplus S_n(5-8)\right) \tag{8}$$

Here, h' is identical to h of Eq. (1). Therefore, random shares (R_k) are generated during the recovery phase by following Eq. (2) to Eq. (5).

2.3.2. *Decryption of Secret Images*

Meaningful shares and generated random shares together reconstruct secret images. Theoretically, the cover image and secret image cannot be completely embedded in a meaningful share. Therefore, the high nibble of these images are utilized to generate meaningful shares. Since the low nibble of secret images are not transmitted, they are randomly generated during reconstruction. The decryption procedure is as follows:

$$\begin{aligned} G'_k(1-4) &\leftarrow Random(1-4) \\ G'_k(5-8) &\leftarrow S_k(1-4) \oplus S_k(5-8) \oplus R_k \end{aligned} \tag{9}$$

For two meaningful shares, G'_1 and G'_2 the values are computed as follows:

$$\begin{aligned} &G'_1(1-4) \leftarrow Random(1-4), \\ &G'_1(5-8) \leftarrow S_1(5-8) \oplus S_1(1-4) \oplus R_1(5-8). \\ &G'_2(1-4) \leftarrow Random(1-4), \\ &G'_2(5-8) \leftarrow S_2(5-8) \oplus S_2(1-4) \oplus R_1(1-4). \end{aligned}$$

Continuing the encoding phase example, where the meaningful share pixel values are S_1 = 123, S_2 = 86, and random share R_1 is 10. Using Eq. (9), reconstructed secret image pixel values are G'_1 = 207 and G'_2 = 144. Here, when the secret image pixel values are 220 and 148 respectively, the reconstructed image pixel values are 207 and 144 respectively. Therefore, we summarize that the proposed scheme attains high-quality recovery of multiple secret images.

Theorem 2 Revealed secret images G'_k (k = 1, ... , n) reconstructed on the decryption side and secret images G_k are alike, and achieve considerably high PSNR value.

Proof 2 High nibble of reconstructed secret images are identical to high nibble of secret images, whereas random generation of low nibble causes dissimilar values. The scenario is the same as explained in Theorem 1 between S_k and C_k. Thus, Theorem 1 corroborates similarity of G'_k and G_k. Theoretical analysis of G'_k and G_k indicates that the worst-case PSNR value is 24.61 dB, while the average PSNR value is 30.63 dB.

2.4 Secret Image Decryption Algorithm

The decryption algorithm shows the procedure to reveal n reconstructed secret images from the n meaningful shares. The decryption Algorithm 2 is as follows.

Algorithm 2: Algorithm for secret image decryption

Input : n meaningful share images (S_k) of size $M \times M$
Output : n reconstructed secret images G'_k of size $M \times M$
Define: m is a bit number, $G_k'^{(m)}(i,j)$ = lower nibble of reconstructed image k at (i, j), $Random_k^{(m)}(i,j)$ = lower nibble of intermediate share image k at (i, j) $G_k'^{(m+4)}(i,j)$ = higher nibble of reconstructed image k at (i, j), $S_k^{(m)}(i,j)$ = lower nibble of meaningful share image k at (i, j), $S_k^{(m+4)}(i,j)$ = higher nibble of meaningful share image k at (i, j)

```
for n ← 1 to k do
  for i ← 1 to M do
    for j ← 1 to M do
      // Generate intermediate random shares R_k
        Follow the Eq. (8) to generate h'
        Generate shares R_k using h' and Eq. (2) to Eq. (5)
      // Generate reconstructed secret images
        for m ← 1 to 4
          G'_k^(m)(i,j) ← Random_k^(m)(i,j)
          G'_k^(m+4)(i,j) ← S_k^(m)(i,j) ⊕ S_k^(m+4)(i,j) ⊕ R_k
      end for
    end for
  end for
end for
return G'_k
```

3 Experimental Results and Analysis

3.1 Experimental Results

Experimental results using a set of different secret images for grayscale and color images are shown in Figure 1 and Figure 2 respectively. All experiments were conducted on 512∗512 images using MATLAB R2016, running on a system with an Intel Core i5 processor and 6 GB of RAM. Figure 1 (*a*) – (*c*) shows three grayscale secret images G_1–G_3 and (*d*) – (*f*) shows three grayscale cover images C_1 – C_3. Generated meaningful shares S_1 – S_3 using the proposed method are shown in Figure 1 (*g*) – (*i*), respectively. Figure 1 (*j*) – (*l*) represents the revealed secret images $G'_1 - G'_3$ after decryption of meaningful shares. Similarly, Figure 2 shows experimental results for color images. Figure 2 (*a*) – (*b*) represents two color secret images G_1 – G_2, (*c*) – (*d*) are color cover images C_1 – C_2, generated meaningful shares S_1 – S_2 using the proposed method are shown in (*e*) – (*f*), and (*j*) – (*h*) presents revealed secret images $G'_1 - G'_2$ after meaningful share decryption.

3.2 Assessment of Threshold Security Criteria

A secret image with substantial regions of similar grayscale intensity values is vulnerable to the threshold security of the scheme. Threshold security is considered compromised if one can recover partial information of secret images from $n - 1$ shares. Chen et al. [4] exhibited computer—synthesized images containing large areas of the same intensity values. Their results show non-correlation between original and shared images. In the proposed scheme, computer—synthesized images are generated to verify the threshold security criteria. Figure 3a–c represents three computer—synthesized images G_1 – G_3 and (d,f) represents three grayscale cover images C_1 – C_3. Generated meaningful shares S_1 – S_3 using the proposed method are shown in Figures 3(g)–(i), whereas (j)–(l) represents revealed secret images $G'_1 - G'_3$ after decryption of meaningful shares. Here, the meaningful share images S_1–S_3 do not disclose any information about the secret images G_1–G_3, despite the latter containing segments of same intensity values. Moreover, meaningful shares contain encrypted content of secret images and are not possible to decrypt from $n-1$ shares. Hence, non-association between meaningful share images and secret images shows the proposed scheme satisfies threshold security criteria.

3.3 Imperceptibility Analysis

The imperceptibility parameter falls within the acceptable range in terms of PSNR [21]. High imperceptibility between meaningful share and cover images indicates a high visual quality of the meaningful shares, whereas high perceptibility between secret and reconstructed images shows high contrast of recovered images. Objective or mathematical analysis of imperceptibility is conducted using PSNR. Average PSNR value between meaningful share and cover images for grayscale images of Figure 1 is 32.97 dB. Similar comparison for color images of Figure 2 is 31.77 dB. Moreover, the average PSNR value between secret and recovered images for grayscale images in Figure 1 is 34.72 dB, and for color images in Figure 2, the PSNR value is 32.25 dB. In meaningful MSS schemes, there is a trade-off between the recovered image and the share image. Notably, the PSNR of the recovered and share images in the proposed scheme exceeds 30 dB, indicating high-quality of reconstruction and meaningful shares.

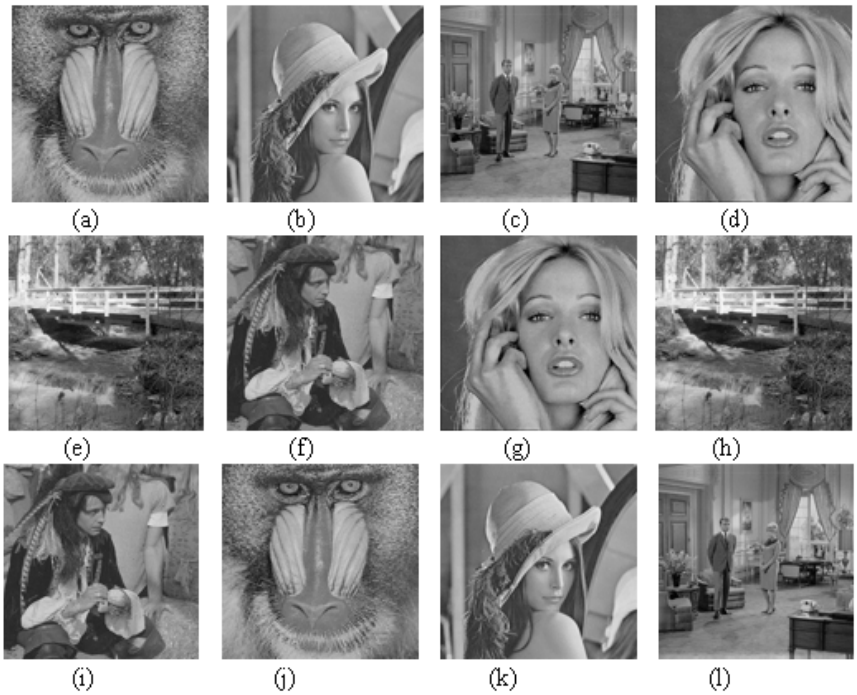

Figure 1. Proposed (3,3) MSS meaningful scheme for grayscale images (a)–(c) Secret images G_1–G_3. (d)–(f) Cover images C_1–C_3. (g)–(i) Meaningful share images S_1–S_3. (j)–(l) Recovered secret images $G_1' - G_3'$.

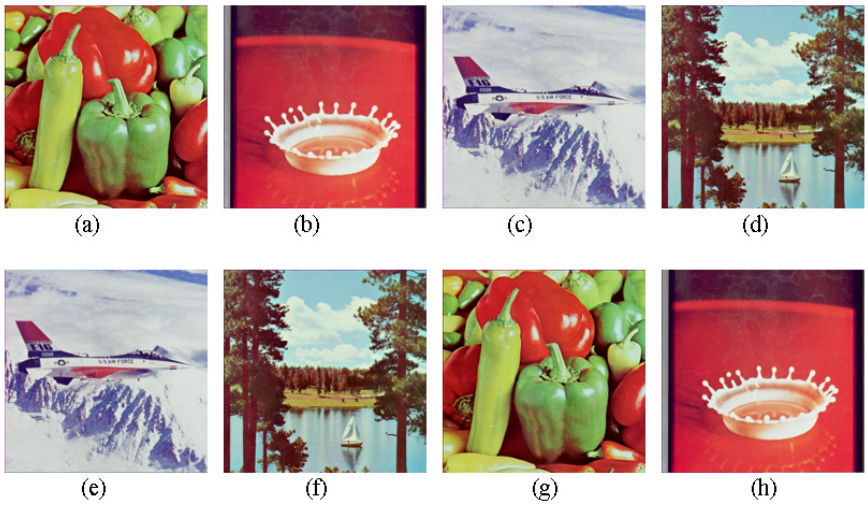

Figure 2. Proposed (2,2) MSS meaningful scheme for color images (a, b) Secret images G_1 and G_2. (c, d) Cover images C_1–C_2. (e, f) Meaningful share images S_1–S_2. (g, h) Recovered secret images G_1' and G_2'.

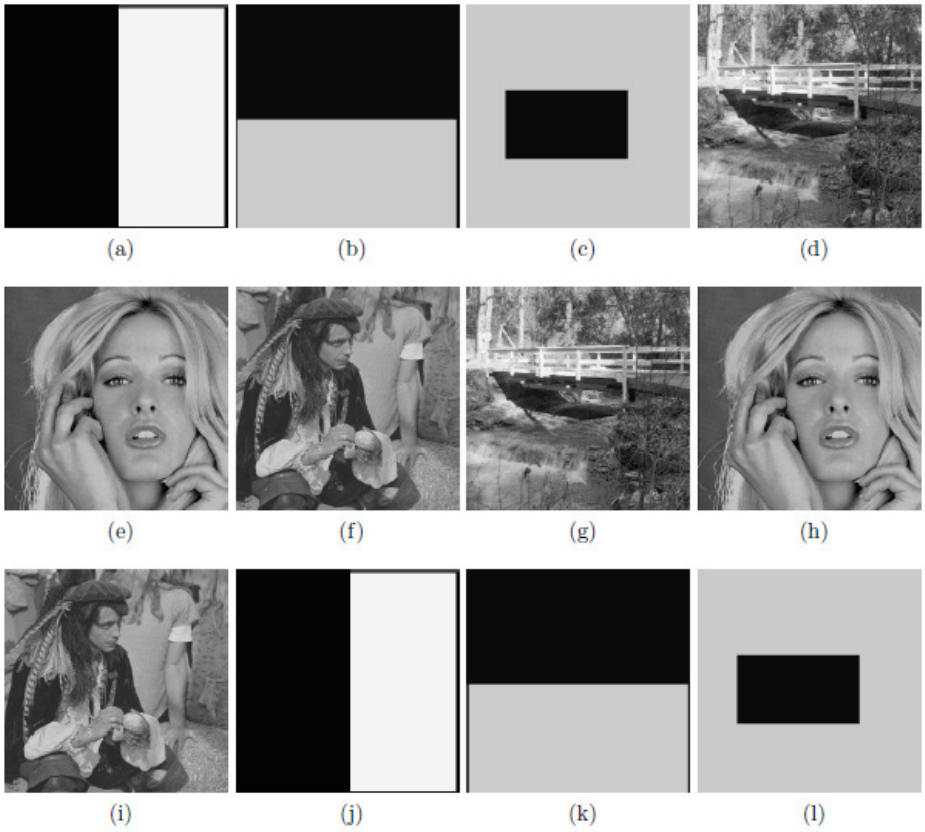

Figure 3. Proposed MSS meaningful scheme for computer-synthesized images. (a)–(c) Secret images G_1–G_3. (d)–(f) Cover images C_1–C_3. (g)–(i) Meaningful share images S_1–S_3. (j)–(l) Recovered secret images $G_1' - G_3'$.

3.4 Performance Analysis

Sharing Capacity: Sharing capacity is an important efficiency performance parameter relating secret images, share images, and pixel expansion. The sharing capacity is defined as [1, 27]:

$$\frac{Number\ of\ secret\ images}{Number\ of\ the\ share\ images * Pixel\ exppansion} \tag{10}$$

A higher value of sharing capacity indicates greater efficiency. Typically, it is limited to 1. In the proposed scheme, the size of all meaningful share images is the same as the size of secret images. Hence, it offers a pixel expansion as 1. Moreover, our scheme requires *n* meaningful shares to transmit *n* secret images. Therefore, the proposed scheme achieves optimum sharing capacity of 1 and is a highly efficient scheme. Notably, the proposed scheme has meaningful shares with improved contrast compared to other schemes. We have utilized a nibble for hiding encrypted secret and a nibble for cover image without utilizing any additional share. Though improved sharing capacity seems very trivial in nature, it is significant especially when the number of shares is small, which is a common scenario. For example, while sharing 2 secret images, (*n, n* +1) schemes require 3 shares whereas the proposed scheme requires 2 shares only and hence, improves the sharing capacity by 33.33%. Similarly, for 3 secret images, it improves by 25%.

Hiding Capacity: The hiding capacity is defined as [1, 27],

$$\frac{The\ size\ of\ secret\ images}{The\ size\ of\ cover\ images} \tag{11}$$

In addition to image sharing applications, the proposed scheme can also be used in image hiding schemes [1, 27]. As the size of secret images and cover images is same, the hiding capacity of the proposed scheme is also 1. The high sharing capacity and high hiding capacity of the proposed scheme reduce storage burden and transmission bandwidth.

Management Efficiency: Management efficiency term is introduced by Yan et al. [17] which means meaningful cover images increase management efficiency and decrease suspicion. Furthermore, a higher sharing capacity also increases management efficiency. As the proposed scheme requires *n* shares to share *n* secret images and has all meaningful shares, it offers high management efficiency compared to schemes that (i) use meaningless shares and (ii) provide a sharing capacity less than 1.

Computational Complexity: Encryption and decryption involve SHA-256 algorithm, circular padding, Torus automorphism, modulo operation, circular left shift operation, and XOR operations. The computational complexity of each function but SHA-256 is O (M ∗ M), while for SHA-256, it is O (1). Hence, for *n* secret images, computational complexity is n ∗ [(5 ∗ O (M ∗ M)) + O (1)].

Limitations: The proposed scheme utilizes a nibble for hiding an encrypted secret and a nibble for cover image without utilizing any additional share. The proposed scheme ensures high-quality reconstruction and meaningful shares and cannot be distinguished by the human visual system. However, it is inherently constrained in achieving lossless reconstruction.

3.5 Security Analysis

Security of the proposed scheme is also analyzed using brute-force attack. Brute-force attack is a comprehensive trial and error method to decrypt data using all possible combinations. In VSS or MSS schemes where images are utilized, the search space for brute-force attacks increases manifold. Single grayscale image of size $M * M$ has 8^{M*M} different possible solutions. Grayscale image of size 512 ∗ 512 has $8^{512*512}$ possible combinations. Thus, the proposed method fulfills security condition as it is not feasible to extract information using brute-force.

Another threat to the proposed scheme is that an attacker could recover the secret image *k* by guessing the value of h' if the attacker obtains share *k*. Here, h' can be calculated only if all shares are available. Alternatively, h' can be obtained by applying brute – force attack with 2^{256} or $1.16 * 10^{77}$ attempts. Even if we consider guessing h' by breaking SHA256 algorithm, to reveal a secret image requires circular padding, Torus automorphism, modulo operation, circular left shift operation, and XOR operation for each 2^{256} possibilities of h'. VSS schemes are kind of one-time pad (OTP) schemes. Even though we consider that the intruder has a copy of a genuine share and all operations are performed in the limited duration, only a single secret will be revealed. However, practically it is not feasible and the proposed scheme fulfills the security criteria.

3.6 Information Entropy Evaluation

The entropy can be used to measure the randomness of the share images. Higher entropy leads to increased randomness which ensures that the share looks random and reveals no information about the secret image. In-formation entropy is defined as,

$$H = \sum_{z=0}^{255} \left(p(z) * \log_2 p(z) \right) \tag{12}$$

where, z = pixel values, ranges between 0 to 255 for 8-bit grayscale image $p(z)$ = probability of each pixel value z, H = entropy in bits /pixel

To ensure the randomness of the shares, entropy calculation is carried out for three meaningful share images of Figure 1. For a grayscale image, the maximum entropy value is 8, while values between 6 and 8 are regarded as high entropy. Experimental results exhibit entropy values for Figure 1g–i as 7.17, 7.72, and 7.38 respectively with an average entropy value as 7.42. High entropy value of the experimental results validates the share security of the proposed scheme.

4 Comparison and Discussion

The comparison between the proposed scheme and related MSS schemes is based on type of image, symmetric function, sharing capacity, quality of recovery, share type, and management efficiency. Type of image represents different image formats supported by the scheme, like binary or gray. Symmetric function indicates use of identical function in sharing and recovery procedures [4]. Symmetric function helps in system development by reducing implementation overhead. Table 1 illustrates the comparison of related MSS schemes with the proposed scheme. Though Chen and Wu scheme [1] supports binary and gray secret image type and provides lossless reconstruction of secret images, their scheme has low

sharing capacity and does not fulfill symmetric function criteria. Refs. [2] and [3] have high sharing capacity but do not have symmetric function. Management efficiency of the related MSS schemes [1, 2, 3, 4, 5, 6] is low as their share type is meaningless.

Furthermore, Table 2 shows secret sharing schemes comprise of both meaningful and multiple shares using type of images, decoding method, sharing capacity, average PSNR between meaningful shares and cover images, average PSNR between secret and recovered images, and management efficiency. Schemes [20] and [21] proposed meaningful share-based schemes using Boolean operation for sharing multiple secret images. Here, Reddy and Prasad [20] achieve lossless recovery of secret images using Boolean OR, AND, and XOR operations but their scheme has sharing capacity of (*n,* 3*n*). Likewise, Boolean XOR-based scheme to share multiple secret images proposed by Shivani et al. [21] has lossy share images with an average PSNR of 17.28 dB. Apart from *n* meaningful shares, their scheme requires noise-like secret key share which increases suspicion. Hence, their scheme has a meaningless share and has sharing capacity of (*n, n* + 1).

Compared to [20] and [21], the proposed scheme attains high efficiency in terms of sharing capacity as (*n, n*). The proposed scheme has *n* meaningful share images for sharing *n* secret images and has PSNR greater than 30 dB for meaningful share and recovered images. As reported in [18], images having 30 dB or higher value of PSNR are considered as good visual quality images and cannot be distinguished by the human eyes. Compared to related meaningful share-based MSS schemes, the proposed scheme gets less encoding space due to high sharing capacity. Hence, lossy recovery is inevitable in the proposed scheme while embedding *n* secret and *n* cover images into *n* shares. For example, when secret images are two, scheme with (*n, n* + 1) sharing capacity [21] requires three shares. With one additional share, 33% more encoding space is available. Similarly, scheme with (*n,* 3*n*) sharing capacity [20] requires six shares and has 66% more encoding space.

Though subjective analysis of [21] scheme shows better performance in recovered image quality compared to the proposed scheme, the human eye cannot distinguish between their scheme and the proposed scheme. Whereas, subjective and objective analyses of [21] show poor visual quality of shares compared to the proposed scheme as meaningful shares of [21] have average PSNR of 17.28 dB compared to 33 dB of the proposed scheme. Furthermore, management efficiency of the proposed scheme is higher compared to [20] and [21].

Ref. [24] proposed a meaningful multi-secret sharing scheme using random grids. Though their scheme can share *n* secret images using 2 shares, their scheme has poor PSNR of share images and low visual quality of recovered image. Moreover, their scheme supports only binary format as decoding of their scheme uses a human visual system. Recent research in the meaningful multi-secret sharing scheme is based on XOR Boolean operation [23]. Visual quality of their proposed scheme varies with the introduction of two new parameters, the number of pieces and proportion of pixels that are camouflaged in a share. Moreover, this scheme suffers from poor visual quality of shares and recovered images. Furthermore, the scheme supports only binary format.

5 Conclusion

This manuscript describes an efficient (*n, n*) multiple secret sharing scheme with improved sharing capacity and enhanced meaningful share image quality besides reconstructed secret image quality. In addition to generating meaningful shares, the sharing process conceals the content of secret images to enhance the security of the shared images. The randomness of shares is ensured by using Boolean XOR, torus automorphism, the secure hash algorithm (SHA-256), and bit shift functions. The potential threat of obtaining h' through a brute-force attack is also analyzed. Notably, these random shares are not transmitted; only meaningful shares need to be shared. An equal number of share and secret images improves the sharing capacity of the scheme to (*n, n*), which, in turn, enhances efficiency. Moreover, PSNR values exceeding 30 dB for meaningful share images and reconstructed secret images indicate the improved visual quality of the proposed scheme. Thus, this study highlights the advantages of the proposed scheme over previous schemes as: high sharing capacity for multiple secret images and improved quality of both meaningful share images and reconstructed secret images.

Table 1. Comparison between Related MSS Schemes and the Proposed Scheme.

	Type of image	**Symmetric function**	**Sharing capacity**	**Quality of recovery**	**Share type**	**Management efficiency**
[1]	Binary, Gray	No	$(n, n+1)$	Lossless	Meaningless	Low
[2]	Gray	No	(n, n)	Lossless	Meaningless	Low
[3]	Gray	No	(n, n)	Lossless	Meaningless	Low
[4]	Gray	Yes	(n, n)	High quality	Meaningless	Low
[5]	Gray	Yes	(t, n) GAS	Lossless	Meaningless	Low
[6]	Gray	Yes	(n, n)	Lossless	Meaningless	Low
The Proposed Scheme	Gray	Yes	(n, n)	High quality	Meaningful	High

Table 2. Comparison between Related Meaningful and Multiple Share-based MSS Schemes and the Proposed Scheme.

Parameters	**[20]**	**[21]**	**[24]**	**[23]**	**The Proposed Scheme**
Type of image	Gray	Gray	Binary	Binary	Gray
Decoding method	Boolean [OR, AND, XOR]	Boolean [XOR]	Random grid	Boolean [XOR]	Boolean [XOR]
Sharing capacity Share type	$(n, 3n)$ Meaningful	$(n, n+1)$ Meaningful and Meaningless	$(n, 2)$ Meaningful	(n, n) Meaningful	(n, n) Meaningful
Average PSNR between meaningful shares and cover images	57 dB ($2n$ shares), Infinity (n shares)	17.28 dB	< 11 dB	< 10 dB	33 dB
Average PSNR between secret and recovered images	Infinity	68 dB	Low	< 22 dB	34.72 dB
Management efficiency	Low	Low	High	High	High

Author Contributions

Conceptualization, Y.M.; methodology, Y.M., V.K., and L.D.; software, V.K.; validation, Y.M. and V.K.; formal analysis, Y.M. and V.K.; investigation, V.K.; resources, Y.M. and V.K.; writing—original draft preparation, V.K.; writing—review and editing, L.D. and Y.M.; supervision, Y.M. All authors have read and agreed to the published version of the manuscript. Authorship must be limited to those who have contributed substantially to the work reported.

Funding

This research received no external funding.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Data Availability Statement

No datasets were generated or analyzed during the current study.

References

[1] Chen, T.H., Wu, C.S.: Efficient multi-secret image sharing based on Boolean operations. Signal Processing 91(1), 90–97 (2011)

[2] Chen, C.C., Wu, W.J.: A secure Boolean-based multi-secret image sharing scheme. Journal of Systems and Software 92, 107–114 (2014)

[3] Yang, C.N., Chen, C.H., Cai, S.R.: Enhanced Boolean-based multi secret image sharing scheme. Journal of Systems and Software 116, 22–34 (2016)

[4] Chen, C.C., Wu, W.J., Chen, J.L.: Highly efficient and secure multi-secret image sharing scheme. Multimedia Tools and Applications 75(12), 7113–7128 (2016)

[5] Nag, A., Singh, J.P., Singh, A.K.: An efficient boolean based multi-secret image sharing scheme. Multimedia tools and applications 79, 16219–16243 (2020)

[6] Chattopadhyay, A.K., Nag, A., Singh, J.P., Singh, A.K.: A verifiable multi-secret image sharing scheme using XOR operation and hash function. Multimedia Tools and Applications 80, 35051–35080 (2021)

[7] Bisht, K., Deshmukh, M.: A novel approach for multilevel multi-secret image sharing scheme. The Journal of Supercomputing 77(10), 12157–12191 (2021)

[8] Rawat, A.S., Deshmukh, M., Singh, M.: A novel multi secret image sharing scheme for different dimension secrets. Multimedia Tools and Applications 82(23), 35183–35219 (2023)

[9] Chattopadhyay, A.K., Saha, S., Nag, A., Singh, J.P.: A verifiable multi-secret image sharing scheme based on DNA encryption. Multimedia Tools and Applications pp. 1–17 (2024)

[10] Surekha, B., Swamy, G., Rao, K.S., Kumar, A.R.: A watermarking technique based on visual cryptography. Journal of Information Assurance and Security 4(6), 470–473 (2009)

[11] Hiwarekar, A.: New mathematical modeling for cryptography. Journal of Information Assurance and Security 9(2014), 027–033 (2014)

[12] Gaidarski, I., Minchev, Z., Andreev, R.: Model driven approach for designing of information security system. Journal of Information Assurance and Security 13, 154–110 (2019)

[13] Hou, Y.C., Wei, S.C., Lin, C.Y.: Random-grid-based visual cryptography schemes. IEEE Transactions on Circuits and Systems for Video Technology 24(5), 733–744 (2014)

[14] Chen, Y.H., Juan, J.S.T.: XOR-based (n, n) visual cryptography schemes for grayscale or color images with meaningful shares. Applied Sciences 12(19), 10096 (2022)

[15] Gao, K., Horng, J.H., Chang, C.C.: An authenticatable (2, 3) secret sharing scheme using meaningful share images based on hybrid fractal matrix. IEEE Access 9, 50112–50125 (2021)

[16] Yadav, M., Singh, R.: Essential secret image sharing approach with same size of meaningful shares. Multimedia Tools and Applications 81(16), 22677–22694 (2022)

[17] Yan, X., Lu, Y., Lu, L.: General meaningful shadow construction in secret image sharing. IEEE Access 6, 45246–45255 (2018)

[18] Li, X.S., Chang, C.C., He, M.X., Lin, C.C.: A lightweight untraceable visual secret sharing scheme based on turtle shell structure matrix. Multimedia Tools and Applications 79(1), 453–476 (2020)

[19] Kapadiya, V.J., Desai, L.S., Meghrajani, Y.K.: Visual secret sharing technique for meaningful shares using Boolean operation. In: Proceedings of 2018 International Conference on Advanced Computation and Telecommunication (ICACT). pp. 249–257. IEEE (2018)

[20] Reddy, L.S., Prasad, M.V.: Extended visual cryptography scheme for multi-secret sharing. In: Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics. pp. 249–257. Springer (2016)

[21] Shivani, S., Ragitha, R., Agrawal, S.: XOR-based continuous-tone multi secret sharing for store-and-forward telemedicine. Multimedia Tools and Applications 76(3), 3851–3870 (2017)

[22] Kapadiya, V.J., Desai, L.S., Meghrajani, Y.K.: Boolean-based multi secret sharing scheme using meaningful shares. In: 2nd International Conference on Innovative Communication and Computational Technologies (ICICCT). pp. 840–844. IEEE (2018)

[23] Huang, S.Y., Lo, A.H., Juan, J.S.T.: XOR-based meaningful (n, n) visual multi-secrets sharing scheme. Applied Sciences 12(20), 10368 (2022)

[24] Huang, B.Y., Juan, J.S.T.: Flexible meaningful multi-secret sharing scheme by random grids. Multimedia Tools and Applications 79(11-12), 7705–7729 (2020)

[25] Meghrajani, Y.K., Desai, L.S., Mazumdar, H.S.: Secure and efficient arithmetic-based multi-secret image sharing scheme using universal share. Journal of Information Security and Applications 47, 267–274 (2019)

[26] Deshmukh, M., Nain, M., Ahmed, M.: Efficient and secure multi secret sharing schemes based on Boolean XOR and arithmetic modulo. Multimedia Tools and Applications 77(1), 89–107 (2018)

[27] Singh, P., Raman, B., Misra, M.: A (n, n) threshold non-expandable XOR-based visual cryptography with unique meaningful shares. Signal Processing 142, 301–319 (2018)