INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Lock and Key Share Secret Sharing Scheme with Meaningful Shares for Grayscale Image and Color Image

Dipak K Rabari[1]*, Yogesh K Meghrajani[1], Laxmi S Desai[2]

1 Department of Electronics & Communication Engg, Dharmsinh Desai University, Nadiad, Gujarat, India
2 Department of Mathematics, Dharmsinh Desai University, Nadiad, Gujarat, India

OPEN ACCESS

Received: 07-08-2024

Accepted: 14-10-2024

Published: 20-11-2024

Citation: Rabari DK, Meghrajani YK, Desai LS (2024) Lock and Key Share Secret Sharing Scheme with Meaningful Shares for Grayscale Image and Color Image. Indian Journal of Science and Technology 17(42): 4405-4414. https://doi.org/10.17485/IJST/v17i42.2486

* **Corresponding author**.

dipakrabari.ec@ddu.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The proposed scheme aims to present a secret sharing scheme (2, m, n) with lock and key shares, including meaningful shares for all lock and key shares. **Methods:** To create m lock and n key shares, the secret image will be encrypted. To retrieve the secret information from the recipient, any one share from the lock and another share from the key shares are used. When both shares are selected from either lock shares or key shares, no partial information about the hidden image is recovered. Meaningful shares do not disclose any information on the privacy of the picture data. The secret image at the recipient can have lossless reconstruction with minimal computation. **Findings:** The performance analysis of a proposed minimally computational secret sharing approach shows the structural similarity index (SSIM) as 1 and correlation as 1 which yields a reconstructed image that is exactly the same as the secret image. Typically, the secret image is reconstructed from meaningless shares using Boolean XOR. However, because attackers believe that secret information is concealed in meaningless shares, these shares are susceptible to share security breaches. Therefore, meaningful shares will improve the security of the share image. **Novelty:** The scheme provides a two-tier security model with meaningful shares for the secret image formats like grayscale and color images.

Keywords: Visual cryptography; Meaningful shares; Two-tier security; Boolean operation; Information security

1 Introduction

The rapid growth of the Internet facilitates human beings with ease of service in all major sectors. Nowadays, every individual aims to get digital services that result from the processing of information with electronic gadgets. Information security is a major concern of research. In the realm of data security, two fundamental methods exist to guarantee that only authorized recipients can access the intended data: steganography and cryptography. Data security is accomplished by steganography-based approach, cryptography- based approach, and incorporating both approaches. A cryptography-

based solution proposed by Adi Shamir [1] was further extended to visual cryptography by Naor and Shamir [2]. The encryption of secret images in shadow images known as shares is accomplished through the use of visual cryptography or visual secret sharing (VSS) techniques, where each user receives a share. The recovery of the concealed image is feasible by stacking shares of specified users if there is no computational device. Alternatively, when the computational device is present, minimal computation is required to disclose the secret.

1.1 Review of associated VSS schemes

Traditional VSS scheme; proposed by Naor and Shamir [2], encodes a secret image into n noise-like images that are known as meaningless shares. Stacking of k shares is employed at the receiver side where human vision is utilized to retrieve the secret image. Retrieval of a secret image is not possible when stacking operation is performed with k-1 or fewer shares. The research gaps of the existing (k, n) scheme are inferior visual quality or contrast, pixel expansion, requirement of the codebook, and pixel alignment. Random grid (RG)-based VSS scheme has advantages compared to (k, n) scheme, namely no pixel expansion and does not require a codebook. However, inferior visual quality and pixel alignment issues persist in their scheme. Moreover, the RG-based (n, n) and (2, n) are advanced schemes of the Kafri and Keren [3]. All n shares are needed for the decoding of (n, n) scheme, whereas 2 shares are required in (2, n) scheme. Threshold (k, n) scheme based on RG uses mandatory k shares for decryption. Boolean-based VSS scheme resolves the limitations of pixel alignment and lower contrast issues. Loss of contrast is inevitable in classical VSS schemes.

Little computation using computational devices like computer, tablet, or a mobile phone, is applied on noisy shares for retrieval of the lossless secret image by the Boolean-based schemes. Boolean-based schemes got attention from the researchers as secret and retrieved images are identical. Until now, conventional and Boolean-based schemes are discussed which offer an overview by stacking of shares and lossless reconstruction using little computation respectively.

A novel two-in-one decoding scheme provides dual decoding options to the user. Users can get a preview of the secret when a computational resource is unavailable by stacking of shares. Using computational resources, the operation is performed to get a high contrast secret image. Region incrementing two-in-one decoding scheme was proposed [4] which is based on RG. A two-in-one decoding scheme was proposed [5] which offers a higher visual quality of the recovered secret. VSS schemes are applicable to secure legal asset documents [6], secrecy of medical images [7], enhancing home security [8], and healthcare image security [9–11]. Moreover, recent research presents compressed sensing-based scheme [12], VSS in the encrypted domain [13], Boolean-based secret sharing schemes [14,15],and plain text-based schemes [16].

1.2 Secret sharing schemes with meaningful shares

A breach in the confidentiality of the secret information is the research gap of all previous schemes where share images were meaningless, intruders may suspect the secrecy of secret image. Therefore, meaningful share image-based schemes have emerged where share images look the same as usual grayscale or color images. The extended VSS scheme for natural image employs meaningful shares for the recovery of the secret image. To share secret images, half-tone technique is used [17] for color or grayscale images. Poor contrast is observed in the recovered secret images while stacking the shares. Recent schemes are proposed for lossless recovery of the secret image [18] and Boolean-based VSS [19,20]. Usually, XOR-based VSS schemes are used to enhance the recovered secret image's visual quality. However, if generated shares are meaningless or noisy, they can naturally convey the probability of holding the secrecy of information to the attackers.

To solve this issue, XOR-based meaningful VSS scheme was presented by various researchers [3,21–23], where a secret image was encoded into meaningful shares using a cover image. Recent meaningful share-based scheme [24] adopts integer wavelet transform which provides more embedding capacity. Grayscale visual cryptography scheme [25] proposed recently employs asymmetric key authentication. Moreover, meaningful share-based schemes were proposed [1,7,17,26–29] that offer the improved visual version of the recovered secret image for grayscale and color image.

1.3 (2, m, n) lock and key share-based VSS (LK-VSS) scheme

The secret image is encrypted into two shares and each share is mandatory to retrieve the secret image for (2, 2) traditional VSS schemes. Similarly, in the (k, n) threshold VSS scheme, any k shares from n shares are required to retrieve the secret information. The major research gap of existing schemes is that it has no provision of a two-tier security model where shares from two different hierarchy levels are needed for decryption. To gain a better understanding of the idea of LK-VSS scheme, a simple analogy is presented. Consider an application scenario, where a restricted area can be accessed only by two authorized individuals who have a piece of image called a share. These authorities are from the top management hierarchy of an organization like managers

and assistant managers. The major constraint for the access of the restricted area is, the doors will be opened if shareholders are available, one from each group of managers and assistant managers. The doors will not open if both the persons are available from the same group like two managers or two assistant managers.

To address the above-mentioned issues, (2, m, n) LK-VSS schemes are used where a share is mandatory from the m lock shares and another share is from the n key shares. (2, m, n) LK-VSS scheme is employed to boost the security of (2, n) RG-VSS scheme. A dual sharing model is presented, wherein the initial set of shares is designated as lock shares, while the subsequent set of shares is identified as key shares. Secret image retrieval is possible when any one share from each stage is present. Secret image is not revealed if both shares are utilized from any one stage only. Despite this, their scheme is applicable for binary secret image only and is constructing noisy shares. (2, m, n) LK-VSS scheme is also applicable to multi format secrets like grayscale and color images.

1.4 Research Gap

The research gap of recent VSS schemes[5,14] which adopt the mechanism to encode the secret image into meaningless shares. The randomness of these shares creates suspicion to intruders about hiding secret information in the shares. Existing (2, m, n) lock and key share-based secret schemes are available which utilize two shares, one from m lock shares and the other from n key shares to recover the secret image at the receiver. Moreover, major recent schemes generate meaningless share images. This paper presents a novel (2, m, n) LK-VSS scheme for grayscale and color images where meaningful m lock shares and meaningful n key shares are generated with the usage of secret and two cover images. Retrieval of the secret image needs two shares, one from each m lock n key shares. Below is a summary of our contributions to the proposed model that addresses the shortcomings of the current schemes.

- The proposed technique implements the meaningful share-based schemes where share images are not noisy and appear natural or normal to the attackers. Espionage does not find the share images suspicious and this way, it significantly protects the encrypted shares compared to meaningless share generation techniques.
- The novelty of the proposed model is that it provides two-tier security which overcomes the research gap of existing schemes[1,3,5,14,21].
- The proposed scheme is the novel approach to design the LK-VSS scheme by generating meaningful shares for multi-format secret images like grayscale and color images.
- The recovery of the lossless secret image at the recipient without pixel expansion problems, minimal computing complexity and attaining necessary secrecy of the shares to the intruders are the key benefits of the proposed system over earlier schemes.

The organization of the subsequent sections of the paper is as outlined below. In Section 2, the proposed scheme is presented. Section 3 demonstrates experimental results, Section 4 exhibits performance analysis, and Section 5 concludes this paper.

2 Methodology

The proposed scheme expands (2, m, n) LK-VSS scheme for grayscale and color secret images using meaningful shares. Two stages of shares exist, m meaningful lock and n meaningful key shares. Decryption of the secret image requires the presence of a single share from both stages. The proposed scheme is applicable for grayscale as well as color secret images.

2.1 Encryption of secret image into lock and key shares

A secret image G and two cover images C_1 and C_2 are used in the encryption algorithm to generate two sets of meaningful shares as m lock and n key shares. Each pixel of a secret image is manipulated with the pixel of cover images to produce encrypted shares. Initially, first x bits (LSB) of the secret image pixel are examined and used to generate LSB of the pixel of generated image R_1. The remaining (8-x) bits of image R_1 is generated from MSB of cover image 1. The replica of the generated image R_1, (m-1) times generates m meaningful lock shares as mentioned in the encryption algorithm. Image R_2 is employed to generate n meaningful key shares. Boolean XOR operation is employed for the generation of the meaningful shares which results by embedding the information of secret image and cover image.

The methodology for the meaningful lock and key share generation is depicted in the architecture of proposed scheme as shown in Figure 1.

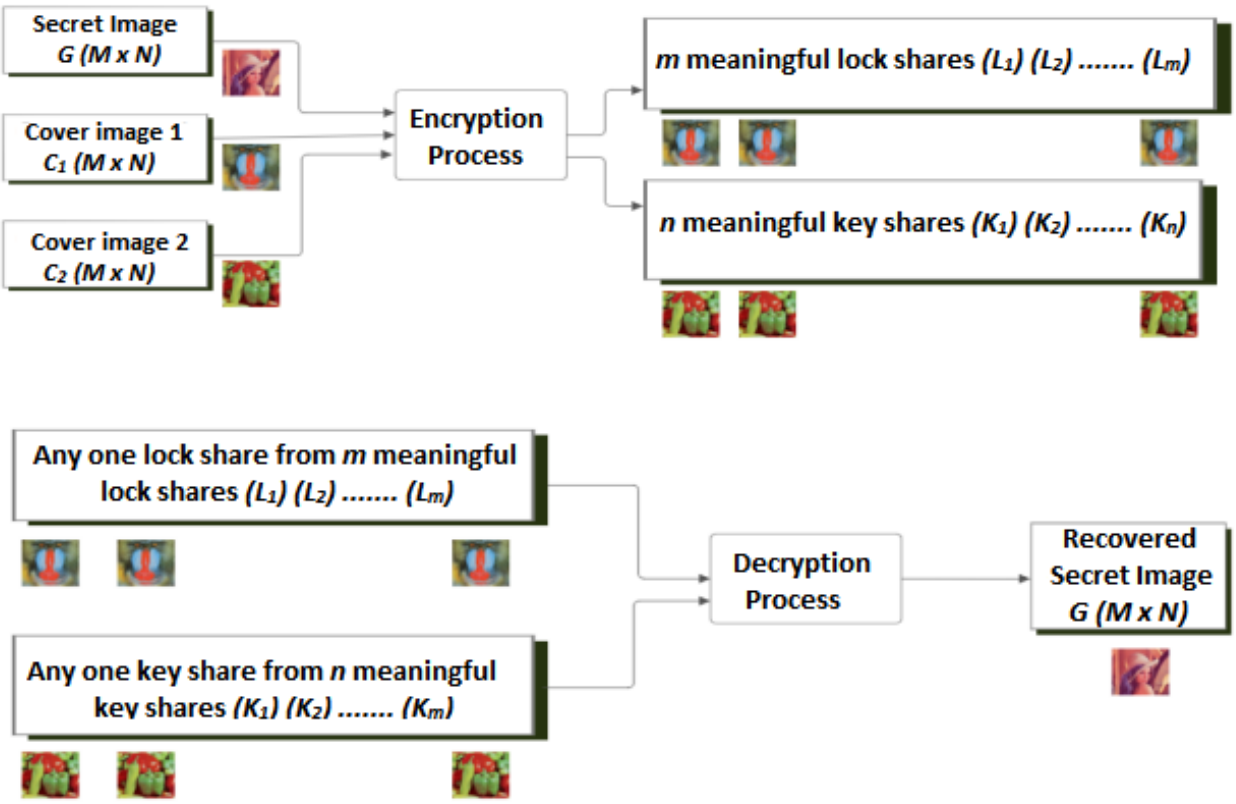

Fig 1. Architecture of the proposed scheme

Encryption algorithm

Input: Grayscale secret image G(M×N), cover images (C_1) (M×N) and (C_2) (M×N)

Output: m meaningful lock shares (L_1) (L_2) .....(L_m) and

n meaningful key shares (K_1) , (K_2).....(K_n)

Step 1: For each pixel [i, j] where $1 \leq i \leq M$, $1 \leq j \leq N$, repeat steps 2 –7.

Step 2: For each secret image pixel [i, j], generate the first x bits (LSB) of R_1(1 to x), where R_1(1 to x) = G(1 to x) and x ∈ {1, 4}.

Step 3: Generate remaining (8-x) bits (MSB) of R_1(x+1 to 8), where R_1(x+1 to 8) = C_1 (x+1 to 8).

Step 4: Compute first x bits (LSB) of R_2(1 to x), where R_2(1 to x) = G (x+1 to 8) ⊕ R_1 (1 to x) where x ∈ {1, 4}.

Step 5: Generate remaining (8-x) bits (MSB) of R_2(x+1 to 8), where R_2(x+1 to 8) = C_2 (x+1 to 8).

Step 6: Replicate value of R_1(i,j) m-1 times to generate m meaningful lock shares as (L_1), (L_2),…..(L_m).

Step 7: Replicate value of R_2(i,j) n-1 times to generate n meaningful key shares as (K_1),(K_2)…..(K_n).

2.2 Decryption of lock and key shares for secret recovery

Operation to decrypt the secret image is Boolean XOR between lock and key shares. The proposed scheme adopts the novel concept of (2, m, n) structure which needs two shares at the receiver to decrypt the secret image. The user selects the first share from m available lock shares and the second share is to be chosen from n key shares. As per the methodology of decryption algorithm, LSB of recovered secret will be generated from LSB of lock share. Moreover, MSB of the revealed secret adopts little computation at the receiver side as mentioned in the algorithm.

Decryption algorithm

Input: m meaningful Lock shares (L_1); (L_2); . . .; (L_m). n meaningful key shares (K_1); (K_2); . . .; (K_n).

Output: Grayscale recovered secret image G'(M×N)

Step 1: Generate first x bits (LSB) of G' (1 to x), where G' (1 to x) = L_i (1 to x) and x ∈ {1, 4}, where i is a lock share from 1, 2, . . . m.

Step 2: Generate remaining (8-x) bits (MSB) of G' (x+1 to 8), where G' (x+1 to 8) = L_i (1 to x) ⊕ K_j (1 to x), where j is a key share from 1, 2,. . n. Here, ⊕ symbolizes Boolean XOR operation.

The scheme adopts XOR-based operation which requires light-weight computations. It provides a two-tier sharing model as security is a prime concern.

- **Lemma 1:** Two shares are needed for the decryption of a secret image at receiver, where any one share from each stage is essential.

Proof: The secret image is retrieved by utilizing two shares at the receiver. The selection of one share from each stage is obligatory. Lock and key shares are represented by L and K respectively. L is any one lock share out of m lock shares denoted as (L_1), (L_2), ..., (L_m). Moreover, K is any one key share out of n key shares denoted as (K_1), (K_2), ...(K_n).

As a case study, consider a scenario where the user selects required share from m lock shares. None of the key share are chosen from n key shares. First x bits (LSB) of recovered secret image G' (1 to x) will be generated from one lock share as mentioned in Equation (1) which is the required methodology of decryption algorithm. However, to generate the remaining (8-x) bits, one lock share from m lock shares and one key share out of n key share is essential as mentioned in the Equation (2). As a consequence, G' (x+1 to 8) will be the XOR operation between two chosen lock shares as shown in Equation (3) which results in G' (x+1 to 8) = 0. Hence, the retrieved image G' does not disclose the secret image as the higher nibble of G' (x+1 to 8) contains no information.

$$G'\ (1\,to\,x) = Li\,(1\,to\,x) \tag{1}$$

$$G'\,(x+1\,to\,8) = Li\,(1\,to\,x) \oplus Kj\,(1\,to\,x) \tag{2}$$

$$G'\,(x+1\,to\,8) = Li\,(1\,to\,x) \oplus Li\,(1\,to\,x) \tag{3}$$

- **Lemma 2:** Shares generated by the proposed scheme which are either lock share or key share represent no information regarding the secret.

Proof: The proposed model constructs m lock and n key shares. As per the encryption algorithm, higher nibble generated in R_1 is similar to C_1. Thus, R_1 looks similar to C_1 as higher nibble contains major information compared to lower nibble. Similarly, R_2 is identical to C_2. Hence, none of the shares discloses any plain information pertaining to the secret image.

Hence, the user cannot recover the secret image if both shares are picked from a stage which is described in Lemma 1. Lemma 2 states that partial information of the secret image is not leaked through any meaningful lock or key share, which fulfills the security criteria of the VSS scheme.

3 Results and Discussion

This section demonstrates simulation outputs of the proposed scheme. We have executed experiments to test the effectiveness of our scheme on 512×512 images with Microsoft Visual C# 2008 with an 11th Gen Intel(R) Core (TM) i3-1115G4 @ 3.00 GHz CPU and 8 GB of RAM. The proposed scheme is implemented for (2, 2, 2) scheme. The secret image of Figure 2**(a)** is encrypted into 2 meaningful lock shares as shown in Figure 2**(d)** - **(e)**. The generated lock share holds the confidentiality of the encrypted share although visually it is similar to the cover image 1. The reason for the visual similarity is demonstrated in the encryption algorithm. Moreover, 2 meaningful key shares are shown in Figure 2**(f)** - **(g)** by embedding the information of two cover images of Figure 2**(b)** - **(c)**. Figure 2 **(h)** illustrates the retrieved image. Similarly, Figure 3 displays the results of the experiment for the secret color image.

The quality assessment of the proposed (2, 2, 2) LK-VSS scheme is shown in Table 1. Figure 4 shows the SSIM and correlation of the proposed (2, 2, 2) LK-VSS scheme. Existing (2, m, n) LK-VSS schemes produce meaningless shares whereas the proposed scheme generates meaningful shares with two in one decoding options. The proposed scheme is assessed with the quality parameters as mentioned below:

Fig 2. (a) Grayscale secret image G (b) Cover image C_1 (c) Cover image C_2 (d) Lock share L_1 (e) Lock share L_2 (f) Key share K_1 (g) Key share K_2 (h) Recovered image G'

3.1 Peak Signal Noise Ratio (PSNR)[1]

The Peak Signal Noise Ratio (PSNR) is an objective evaluation for quality of an image based on the difference in pixel values between two images. A higher PSNR value denotes improved visual quality in the restored image. Mathematically, PSNR is expressed by,

$$PSNR = \left(\frac{MAX^2}{MSE}\right) dB \tag{4}$$

Where MAX=255 for grayscale image and MSE is mean square error which is expressed as

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[X(i,j) - Y(i,j)]^2 \tag{5}$$

Fig 3. (a) Color secret image G (b) Cover image C_1 (c) Cover image C_2 (d) Lock share L_1 (e) Lock share L_2 (f) Key share K_1 (g) Key share K_2 (h) Recovered image G'

3.2 Structural Similarity Index Measure (SSIM)[1]

Structural Similarity Index Measure (SSIM) is utilized to estimate the similarity between two images. Higher SSIM value implies better similarity between two images. For two identical images, SSIM value is 1. It is expressed mathematically as shown below:

$$SSIM_{(x,y)} = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{6}$$

Where μ_x = mean for x, μ_y = mean for y, σ_x^2 = the variance of x, σ_y^2 = variance of y, σ_{xy} = covariance of x and y, $c_1 = (k_1 L)^2$,$c_2 = (k_2 L)^2$ are two variables to stabilize the division with weak denominator, L is the dynamic range of the pixel-values, $k_1 = 0.01$ and $k_2 = 0.03$ by default.

3.3 Correlation [30]

Correlation is a measure to express interrelation between two images. Higher correlation represents closeness of recovered image with original secret image. Correlation is expressed as,

$$\rho(x,y) = \frac{cov(x,y)}{\sigma_x \sigma_y} \tag{7}$$

Table 1. Objective numerical measurement

	Image type	Meaningful share L_1 Vs Cover image C_1	Meaningful share L_2 Vs Cover image C_1	Recovered Image G' Vs Secret Image G
PSNR (dB)	**Grayscale**	31.86	31.78	∞
	Color	31.90	31.56	∞

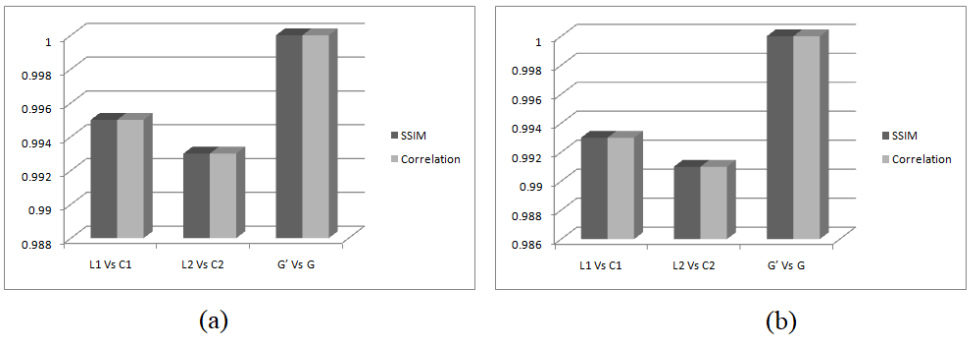

Fig 4. SSIM and correlation analysis (a) grayscale image, (b) color image

Table 2. Comparison between related schemes and the proposed scheme

	Chen and Juan [21]	Wang et. al [5]	Li et. al [1]	Rawat et. al [14]	Mehrnahad et. al [3]	Liu et. al [25]	Proposed Scheme
Image format	Grayscale and color	Grayscale	Color	Grayscale and color	Grayscale	Grayscale	Grayscale and color
Access structure	n, n	k, n	n, n	t, n	n, n	n, n	2, m, n
Recovery strategy	Boolean [XOR]	Two-in-One	Human Visual System (HVS)	Boolean [XOR]	HVS and Boolean [XOR]	OMTAP-VSS	Boolean [XOR]
Number of shares	n shares	n shares	n shares	n shares	n shares	n shares	m lock shares and n key shares
Share type	Meaningful	Meaningless	Meaningful	Meaningless	Meaningful	Meaningful	Meaningful
Pixel alignment issue	No	Yes	No	Yes	No	No	No
Encoding strategy	Boolean [XOR]	Boolean [XOR]	DWT and SVD methods	Boolean [XOR]	Boolean [XOR]	OMTAP-VSS with AEK	Boolean [XOR]
XOR recovery type	Lossless	Lossless	Lossless	Lossless	Lossless	Lossless	Lossless
Two-tier security	No	No	No	No	No	No	**Yes**

Table 1 shows the quality analysis of (2, 2, 2) scheme where PSNR, SSIM, and correlation are calculated between L_1 and C_1, L_2 and C_2, and G and G'. Figure 4 shows the SSIM and correlation of the recovered image with the original secret image. The comparison of our scheme with related schemes [1,3,5,14,21,25] is shown in Table 2. The proposed scheme provides meaningful shares which improve the security aspect of images compared to [5,14]. In comparison with [1,3,5,25], the proposed scheme works on multiple formats of secret image like grayscale and color images. Previous techniques have issues with pixel alignment [5,14], however the suggested scheme is unaffected by this issue. The novelty of the proposed scheme can be stated as it provides a two-tier security model compared to recent innovative schemes [1,3,5,14,21,25] and only two meaningful shares are needed at the receiver instead of n shares compared to [1,3,21,25].

4 Conclusion

Share security is a prime concern in VSS schemes. Existing (2, m, n) LK-VSS schemes generate noisy shares. Hence, the proposed novel scheme offers the advantage of meaningful shares. The major advantage of the proposed model is the security of the shares is improved because the cover image information is extracted in encryption procedure. The PSNR value in Table 1 shows the efficiency of the scheme with 31.86 (L_1 vs C_1) and 31.78 (L_2 vs C_2) for grayscale image. The proposed scheme is applicable to grayscale and color secret images mainly into the environment where two-tier security is a major requirement. The proposed scheme is applicable in a scenario where authorities of an organization want to get access to the restricted area. Lossless recovery of the secret is possible when one share is chosen each from lock shares and key shares. In future, the proposed technique may be enhanced for multi secret LK-VSS with meaningful shares.

References

1) Li W, Peng C, Tan W, Xu Y, Niu K. A reversible and lossless secret image sharing scheme with authentication for color images. *Journal of King Saud University-Computer and Information Sciences*. 2023;35(10):1–10. Available from: https://doi.org/10.1016/j.jksuci.2023.101854.
2) A JB, G SM, S MK. Secured communication method using visual secret sharing scheme for color images. *Journal of Internet Technology*. 2021;22(4):803–810. Available from: https://jit.ndhu.edu.tw/article/view/2544.
3) Mehrnahad Z, Latif AM, Ahmadabadi JZ. A new scheme for lossless meaningful visual secret sharing by using XOR properties. *Journal of AI and Data Mining*. 2023;11:195–211. Available from: https://doi.org/10.22044/jadm.2023.12460.2395.
4) Lin YR, Juan JS. RG-Based Region Incrementing Visual Cryptography with Abilities of OR and XOR Decryption. *Symmetry*. 2024;16:1–27. Available from: https://doi.org/10.3390/sym16020153.
5) Wang X, Li P, Ren Z. Two-in-one secret image sharing scheme with higher visual quality of the previewed image. *Mathematics*. 2022;10(5):1–15. Available from: https://www.mdpi.com/2227-7390/10/5/678.
6) Yamini C, Priya N. Hybrid Encoding Schemes in Image Steganography Combined with Scrambling for Safeguarding Legal Asset Documents. *Indian Journal of Science and Technology*. 2024;17(17):1776–1784. Available from: https://indjst.org/articles/hybrid-encoding-schemes-in-image-steganography-combined-with-scrambling-for-safeguarding-legal-asset-documents.
7) Yan M, Hu Y, Zhang H. Progressive meaningful visual cryptography for secure communication of grayscale medical images. *Multimedia Tools and Applications*. 2024;83:33639–33652. Available from: https://link.springer.com/article/10.1007/s11042-023-16960-z.
8) Mohan J, Rajesh R. Enhancing home security through visual cryptography. *Microprocessors and Microsystems*. 2021;80. Available from: https://doi.org/10.1016/j.micpro.2020.103355.
9) Yan M, Hu Y, Zhang H. Progressive meaningful visual cryptography for secure communication of grayscale medical images. *Multimedia Tools and Applications*. 2023;83(11):33639–33652. Available from: https://dx.doi.org/10.1007/s11042-023-16960-z.
10) Mohammed A, Samundiswary P. SecMISS: Secured Medical Image Secret Sharing mechanism for smart health applications. *The Visual Computer*. 2024;40(6):4251–4271. Available from: https://dx.doi.org/10.1007/s00371-023-03080-w.
11) Al-Haija QA. Biomedical image security. *Advances in Artificial Intelligence*. 2024;p. 561–586. Available from: https://doi.org/10.1016/B978-0-443-19073-5.00007-0.
12) Wu B, Xie D, Chen F, Zhu H, Wang X, Zeng Y. Compressed sensing based visually secure multi-secret image encryption-sharing scheme. *Multimedia Tools and Applications*. 2023;83(7):18919–18941. Available from: https://dx.doi.org/10.1007/s11042-023-15922-9.
13) Wang R, Yang G, Yan X, Luo S, Han Q. Secret image sharing in the encrypted domain. *Journal of Visual Communication and Image Representation*. 2024;98:1–13. Available from: https://dx.doi.org/10.1016/j.jvcir.2023.104013.
14) Rawat AS, Deshmukh M, Singh M. A novel multi secret image sharing scheme for different dimension secrets. *Multimedia Tools and Applications*. 2023;82:1–37. Available from: https://link.springer.com/article/10.1007/s11042-023-14609-5.
15) Lin JY, Horng JH, Chang CC. Secret Image Sharing with Distinct Covers Based on Improved Cycling-Xor. *Journal of Visual Communication and Image Representation*. 2024. Available from: https://www.sciencedirect.com/science/article/abs/pii/S1047320324002384.
16) Maiti C, Dhara BC, Umer S, Asari V. An Efficient and Secure Method of Plaintext-Based Image Encryption Using Fibonacci and Tribonacci Transformations. *IEEE Access*. 2023;11:48421–48440. Available from: https://dx.doi.org/10.1109/access.2023.3276723.
17) Somwanshi DR, Humbe VT. Half-Tone Visual Cryptography Scheme For RGB Color Images. *Indian Journal of Science and Technology*. 2023;16(5):357–366. Available from: https://indjst.org/articles/half-tone-visual-cryptography-scheme-for-rgb-color-images.
18) Luo S, Liu Y, Yan X, Yu Y. Secret image sharing scheme with lossless recovery and high efficiency. *Signal Processing*. 2023;206. Available from: https://dx.doi.org/10.1016/j.sigpro.2023.108931.
19) Wu X, Yao P. Boolean-based Two-in-One Secret Image Sharing by Adaptive Pixel Grouping. *ACM Transactions on Multimedia Computing, Communications, and Applications*. 2023;19(1):1–23. Available from: https://dx.doi.org/10.1145/3517140.

20) Rawat AS, Deshmukh M, Singh M. Natural share-based lightweight (n, n) single secret image sharing scheme using LSB stuffing for medical images. *The Journal of Supercomputing*. 2023;79(17):19138–19167. Available from: https://dx.doi.org/10.1007/s11227-023-05396-9.
21) Huang SY, Lo AH, Juan JS. XOR-based meaningful (n, n) visual multi-secrets sharing schemes. *Applied Sciences*. 2022;12:1–22. Available from: https://doi.org/10.3390/app122010368.
22) Chen YH, Juan JS. XOR-based (n, n) visual cryptography schemes for grayscale or color images with meaningful shares. *Applied Sciences*. 2019;12:1–16. Available from: https://www.mdpi.com/2076-3417/12/19/10096.
23) Kannojia SP, Kumar J. XOR-based unexpanded meaningful visual secret sharing scheme. *International Journal of Security and Networks*. 2019;14(1):1–9. Available from: https://www.researchgate.net/publication/332337527_XOR-based_unexpanded_meaningful_visual_secret_sharing_scheme.
24) Saeidi Z, Mashhadi S. Two meaningful secret image sharing schemes based on integer wavelet transform and LWE. *Computational and Applied Mathematics*. 2024;43(3):1–27. Available from: https://link.springer.com/article/10.1007/s40314-024-02664-z.
25) Liu T, Vairagar S, Adagale S, Karthick T, Karunya CE, A JB, et al. Secure multimedia communication: advanced asymmetric key authentication with grayscale visual cryptography. *Mathematical Biosciences and Engineering*. 2024;21(3):4762–4778. Available from: https://www.aimspress.com/article/doi/10.3934/mbe.2024209?viewType=HTML.
26) Armijo-Correa JO, Murguía JS, Mejía-Carlos M, Arce-Guevara VE, Aboytes-González JA. An improved visually meaningful encrypted image scheme. *Optics & Laser Technology*. 2020;127:159–165. Available from: https://doi.org/10.1016/j.optlastec.2020.106165.
27) Pan JS, Liu T, Yang HM, Yan B, Chu SC, Zhu T. Visual cryptography scheme for secret color images with color QR codes. *Journal of Visual Communication and Image Representation*. 2022;82. Available from: https://doi.org/10.1016/j.jvcir.2021.103405.
28) Shankar K, Taniar D, Yang E, Yi O. Secure and optimal secret sharing scheme for color images. *Mathematics*. 2019;9:1–20. Available from: https://www.mdpi.com/2227-7390/9/19/2360.
29) Panchbhai VV, Varade SW. Enhanced block based progressive visual secret sharing scheme for grayscale and color image. *Multimedia Tools and Applications*. 2024;83:50519–50555. Available from: https://link.springer.com/article/10.1007/s11042-023-17416-0#:~:text=The%20proposed%20scheme%20is%20made,to%20rebuild%20an%20undisclosed%20image.
30) Abu-Faraj MA, Al-Hyari A, Obimbo C, Aldebei K, Altaharwa I, Alqadi Z, et al. Protecting digital images using keys enhanced by 2D chaotic logistic maps. *Cryptography*. 2023;7:1–22. Available from: https://doi.org/10.3390/cryptography7020020.