IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 June 2023, accepted 31 July 2023, date of publication 10 August 2023, date of current version 13 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3304055

SURVEY

Secret Image Sharing Schemes: A Comprehensive Survey

SANCHITA SAHA[1,2], (Member, IEEE), ARUP KUMAR CHATTOPADHYAY[3], (Member, IEEE), ANUP KUMAR BARMAN[1], (Member, IEEE), AMITAVA NAG[1], (Senior Member, IEEE), AND SUKUMAR NANDI[4], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Central Institute of Technology Kokrajhar, Kokrajhar, Assam 783370, India
[2]Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia, West Bengal 721657, India
[3]Indian Institute of Technology Madras, Chennai 600036, India
[4]Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, Guwahati, Assam 781039, India

Corresponding author: Amitava Nag (amitava.nag@cit.ac.in)

This work was supported in part by the Central Institute of Technology Kokrajhar provides fund through Professional Development Allowance (PDA).

ABSTRACT The safeguarding of digitized data against unwanted access and modification has become an issue of utmost importance as a direct result of the rapid development of network technology and internet applications. In response to this challenge, numerous secret image sharing (SIS) schemes have been developed. SIS is a method for protecting sensitive digital images from unauthorized access and alteration. The secret image is fragmented into a large number of arbitrary shares, each of which is designed to prevent the disclosure of any information to the trespassers. In this paper, we present a comprehensive survey of SIS schemes along with their pros and cons. We review various existing verifiable secret image sharing (VSIS) schemes that are immune to different types of cheating. We have identified various aspects of developing secure and efficient SIS schemes. In addition to that, a comparison and contrast of several SIS methodologies based on various properties is included in this survey work. We also highlight some of the applications based on SIS. Finally, we present open challenges and future directions in the field of SIS.

INDEX TERMS Secret sharing, secret image sharing, verifiable secret image sharing.

I. INTRODUCTION

Internet technology is constantly accelerating in the modern era, and the quantity of digital data emitted has skyrocketed. However, the consequences of this expansion include a significant increase in the number of threats to information security. In nearly every industry, the use of digital images has become widespread, ranging from personal use to scientific study. There is a vast amount of information that can be observed in images. Many organizations prefer to store such images, which contain sensitive and confidential data. An industry or organization may want to protect sensitive data from competitors. For instance, it is essential for companies that design jewelry to keep the images of their newest designs secret from rival businesses that might try to replicate or create designs that are similar to these. Due to this, those who design jewelry do their best to prevent any scenario in which their trade secrets could be exposed. Thus, it is necessary to have a high level of security in order to safeguard such sensitive data from being accessed or modified without authorization by intruders. Several techniques like encryption [1], [2], digital watermarking [3], [4] and image steganography [5], [6] are used to improve the security of images that contain sensitive information. However, there are disadvantages to these techniques as the information is contained in a single information carrier. If the information carrier carrying the sensitive information is destroyed by an intruder or if the information carrier itself is lost, then the sensitive information might be lost. In these scenarios, *secret sharing (SS) schemes* offer practical and economical solutions to resolve the issues. Shamir [7] and Blakley [8] were the first to independently introduce two distinct threshold secret sharing (TSS) schemes. Shamir's scheme [7] is based on

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son.

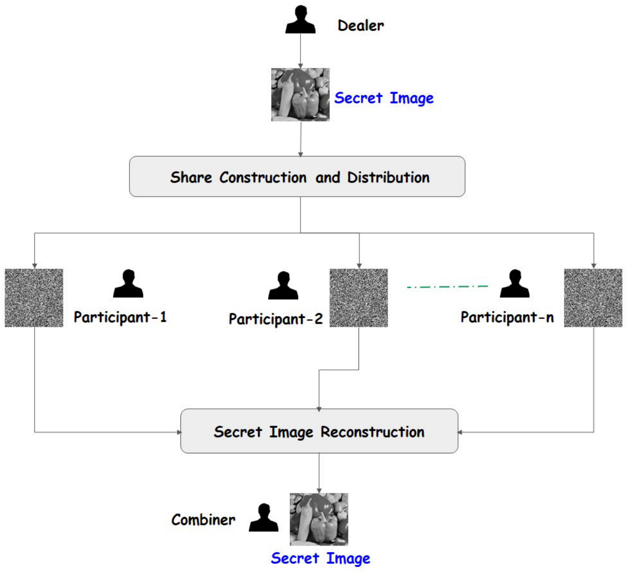


FIGURE 1. Threshold secret sharing.

polynomial interpolation, and Blakley's scheme [8] is based on the concept of hyperplane geometry. Another SS scheme, introduced by Mignotte [9] was improved by Asmuth and Bloom [10] based on the Chinese remainder theorem (CRT). Chum et al. [11] proposed a scheme based on the closest Vector Problem (CVT) [12]. Later, Fine et al. [13] discussed a detailed comparison of Shamir's scheme [7] with the scheme proposed by Chum et al. [11]. Afterward, numerous researchers [14], [15], [16], [17], [18] have extended the scheme proposed by Shamir [7]. Each of the schemes follows the concept of threshold secret sharing (TSS), which is commonly defined as (t, n) - TSS.

In a (t, n) - TSS scheme (as shown in Fig. 1), the owner of the secret or a reliable third party, also known as the dealer, divides a secret into n parts that are referred to as shares (or shadows). The shares are distributed among n number of participants (or players) in such a manner that each of the participants holds exactly one share. Reconstruction of the secret is possible only when an authorized set of participants collaborate to compute the secret with their shares. In a (t, n) threshold secret sharing scheme, the t number (referred to as the threshold value) of shares must be combined to reconstruct the secret. However, the secret can not be reconstructed if the number of shares is less than the threshold t.

The SS schemes can be extended to share one or more secret images. However, the traditional SS schemes are inefficient at sharing secret images. Therefore, a particular class of SS schemes known as *Secret Image Sharing (SIS)* was introduced. The primary kind of SIS scheme is visual secret sharing (VSS) or visual cryptography (VC). On the other hand, several popular SIS schemes exist based on various methods such as polynomial interpolation, XOR operations, CRT methods, etc. A SIS scheme is a technique that can be used to protect a sensitive digital image from being illegally exposed by unauthorized access. Thein and Lin [14] proposed the first SIS scheme based on Shamir's TSS [7]. Afterward, many researchers [19], [20], [21], [22], [23], [24], [25], [26], [27] worked on SIS schemes using different techniques. However, these SIS schemes are open to various types of cheating. Horng et al. [28] initially demonstrated that cheating is practicable in VC and introduced two different approaches to prevent it. Subsequently, several researchers [29], [30], [31], [32], [33] worked on verifiable SIS schemes using different techniques.

There are several real-life applications of SS schemes, such as in IoT, blockchain, secure data outsourcing in the cloud, privacy-preserving big data aggregation in the smart grid, federated learning, electronic voting systems, and threshold cryptography [34], [35], [36], [37], [38], [39], [40], [41]. Secret image sharing (SIS) has also lots of applications, such as QR-codes [42], [43], medical image security [17], [44].

In our other work (communicated), we presented a detailed review of some essential basic TSS schemes, multi-secret sharing schemes, and verifiable secret sharing schemes. In this paper, we provide a comprehensive survey of different SIS schemes, MSIS schemes, and VSIS schemes.

A. MOTIVATION OF THE WORK

Secret Image Sharing (SIS) is an important area of research due to the increasing use of digital images in various applications and the need to protect sensitive images from unauthorized access and distribution. The SIS landscape is rapidly evolving, with new techniques, applications, and challenges emerging. With the increasing use of digital images in various applications, including social media, e-commerce, and entertainment, the need for secure and efficient methods for image sharing is becoming more critical. Sensitive images, such as medical images or scanned copies of government documents, images of military installations, satellite images, court evidence, etc., are prone to illegal access, tampering, and distribution. Secret image sharing techniques can help protect these images from such threats, making them an important area of research. While some existing surveys have focused on specific SIS techniques or applications, there are insufficient comprehensive surveys that provide a holistic view of this field. Therefore, this survey aims to provide a summary of the current state of SIS research, highlight the challenges and gaps in the literature, and compare the strengths and weaknesses of various SIS techniques. The results of this survey can help researchers better understand the evolving SIS landscape and identify areas that require further investigation.

B. SCOPE OF CONTRIBUTIONS

The primary objectives of this survey are outlined below.

- This survey provides a review of the most essential SIS schemes that have been intensively studied and extended by various researchers.

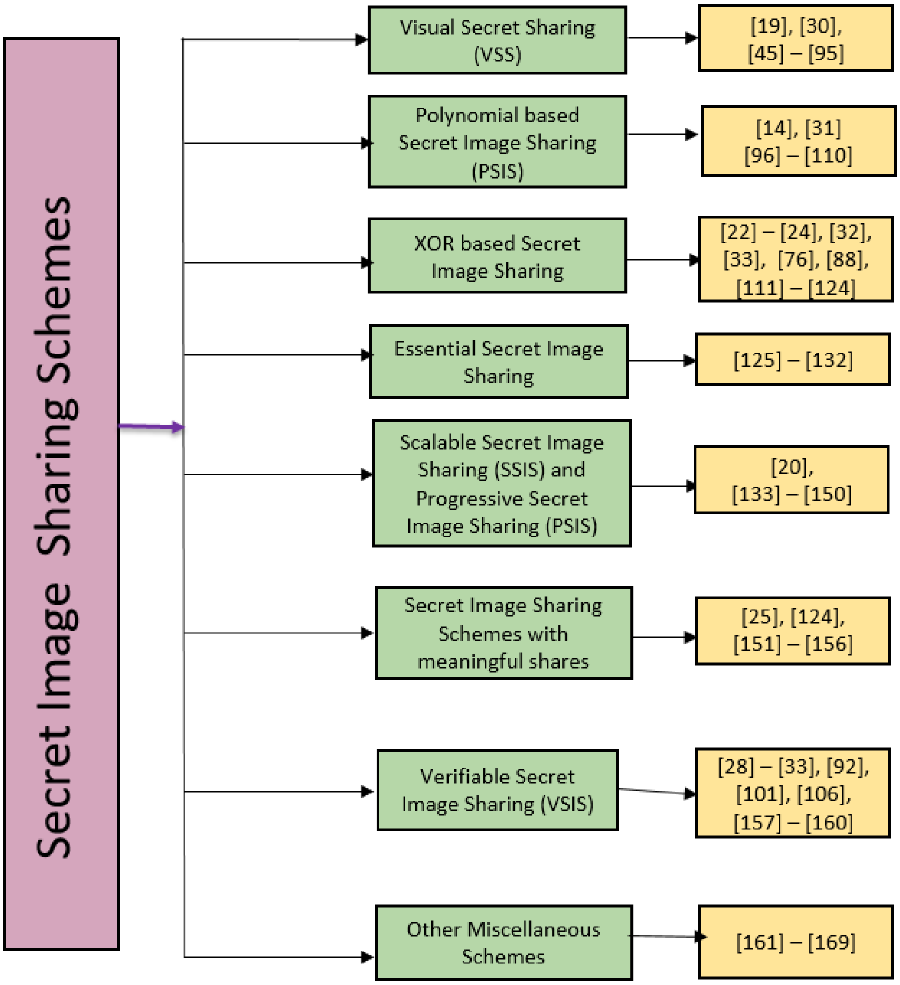

Secret Image Sharing Schemes
Visual Secret Sharing (VSS)
[19], [30], [45] – [95]
Polynomial based Secret Image Sharing (PSIS)
[14], [31] [96] – [110]
XOR based Secret Image Sharing
[22] – [24], [32], [33], [76], [88], [111] – [124]
Essential Secret Image Sharing
[125] – [132]
Scalable Secret Image Sharing (SSIS) and Progressive Secret Image Sharing (PSIS)
[20], [133] – [150]
Secret Image Sharing Schemes with meaningful shares
[25], [124], [151] – [156]
Verifiable Secret Image Sharing (VSIS)
[28] – [33], [92], [101], [106], [157] – [160]
Other Miscellaneous Schemes
[161] – [169]

FIGURE 2. Classification of SIS schemes.

- This survey work discusses a detailed study on various secret image sharing techniques, such as: *Visual Secret Sharing (VSS), Polynomial-based SIS, XOR-based SIS, Essential SIS, Scalable and Progressive SIS, and SIS schemes with meaningful shares.*
- Most secret image sharing systems presume all parties are trustworthy, which is rarely the case. This makes them vulnerable to cheating. This survey reviews verifiable SIS schemes to avoid cheating.
- This study also discusses some of the primary application fields for SIS.
- The survey identifies and discusses the open challenges in the area of SIS.

C. ORGANIZATION OF THE PAPER

The rest of the paper is arranged as follows: In Section II, we discuss some of the preliminaries related to our work. In Section III, a few examples of secret sharing schemes are provided. In Section IV, we provide a detailed review of Shamir's TSS scheme. In Section V, we present a detailed review of basic SIS schemes. In Section VI, we study different types of cheating that can occur during SIS and present review work on VSIS schemes. Section VII presents a study on some of the special types of SIS: *SIS based on cellular automata* and *DNA-based SIS*. Some evaluation matrices of images are discussed in Section VIII. Various SIS-based applications are discussed in Section IX. Section X presents open challenges and future research directions in the field of SIS. Finally, we conclude our work in Section XI. In Fig. 2, we present different varieties of SIS schemes considered in this paper. In Fig. 3, we present the entire structure of the paper.

II. PRELIMINARIES

A. THE ESSENTIAL ENTITIES OF A THRESHOLD SECRET SHARING (TSS) SCHEME

A TSS scheme consists of the following primary entities:

- *Secret:* A secret S is the data that has to be shared among a group of participants.
- *Shares / Shadows:* The secret S is encoded into n shares / shadows, say $s_1, s_2, \cdots, s_n$ in such a manner that any of

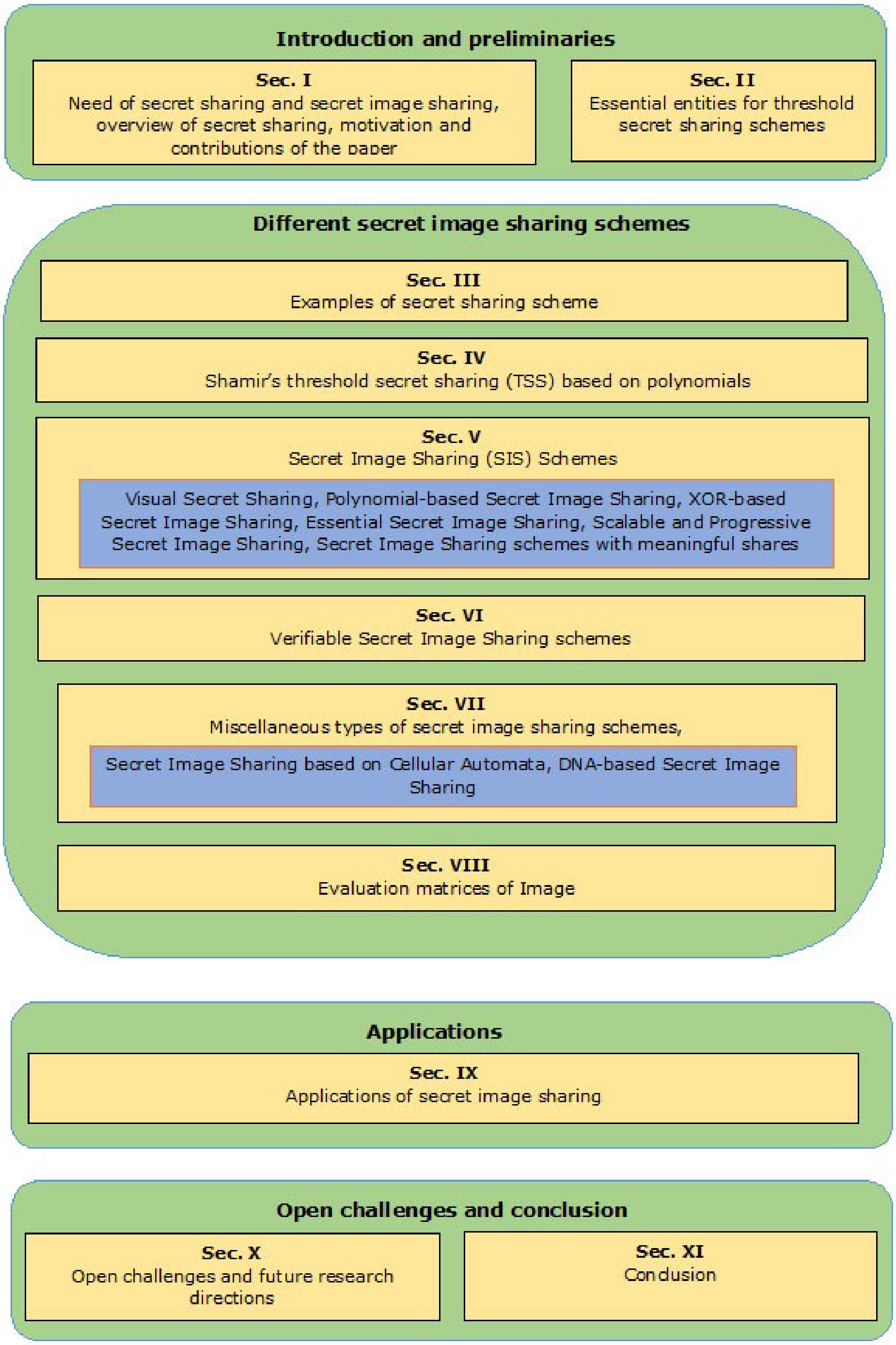

Introduction and preliminaries
Sec. I
Need of secret sharing and secret image sharing, overview of secret sharing, motivation and contributions of the paper
Sec. II
Essential entities for threshold secret sharing schemes
Different secret image sharing schemes
Sec. III
Examples of secret sharing scheme
Sec. IV
Shamir's threshold secret sharing (TSS) based on polynomials
Sec. V
Secret Image Sharing (SIS) Schemes
Visual Secret Sharing, Polynomial-based Secret Image Sharing, XOR-based Secret Image Sharing, Essential Secret Image Sharing, Scalable and Progressive Secret Image Sharing, Secret Image Sharing schemes with meaningful shares
Sec. VI
Verifiable Secret Image Sharing schemes
Sec. VII
Miscellaneous types of secret image sharing schemes,
Secret Image Sharing based on Cellular Automata, DNA-based Secret Image Sharing
Sec. VIII
Evaluation matrices of Image
Applications
Sec. IX
Applications of secret image sharing
Open challenges and conclusion
Sec. X
Open challenges and future research directions
Sec. XI
Conclusion

FIGURE 3. The structure of the article.

these shares alone cannot disclose any information about the secret.

- *Dealer:* Dealer D is responsible for encoding the secret/secrets into n shares/shadows and allocating those shares to the participants such that each participant receives exactly one share/shadow.
- *Participants:* Set $\mathcal{P} = \{P_i\}_{i=1}^{n}$ is used to represent the participants, who obtain the shares from the dealer.
- *Combiner:* A combiner C is in charge of decoding the secret/secrets if an approved subset of participants submits their own shares.

B. ABBREVIATIONS AND SYMBOLS USED IN THE WORK

The different abbreviations and symbols used in this paper are listed in Table 1 and Table 2 respectively.

TABLE 1. List of abbreviations.

Abbreviations	Full Form
CBW-VCS	Color-Black-and-White Visual Cryptography Scheme
CPVSS	Cheating Prevention Visual Secret Sharing
DLP	Discrete Logarithm Problem
MSIS	Multi-Secret Image Sharing
ProbVSS	Probabilistic Visual Secret Sharing
PSIS	Progressive Secret Image Sharing
SIS	Secret Image Sharing
SS	Secret Sharing
SSIS	Scalable Secret Image Sharing
TSS	Threshold Secret Sharing
VC	Visual Cryptography
VSS	Visual Secret Sharing
VSIS	Verifiable Secret Image Sharing
WSIS	Weighted Secret Image Sharing

TABLE 2. List of symbols.

Symbol	Meaning
C	The combiner
D	The dealer
k	Essential participants
n	Number of participants
$P_1, P_2, \cdots, P_n$	The participants
S or $S_1, S_2, \cdots, S_n$	The secret or secrets
$s_1, s_2, \cdots, s_n$	Shares or shadows
t	Threshold of participants

III. EXAMPLES OF SECRET SHARING SCHEME

The following two examples show (4, 4) secret sharing schemes in their simplest form, where there are four participants, and all the participants must submit their shares to reconstruct the secret.

Example 1: The dealer chooses a secret S as an integer. Let it be $S = 108$. He/she further selects three random integers as three shares as: $s_1 = 228$, $s_2 = -365$, $s_3 = 98$, and computes the fourth share s_4 as follows:

$$\begin{aligned} s_4 &= S - (s_1 + s_2 + s_3) \\ &= 108 - (228 + -365 + 98) \\ &= 147 \end{aligned}$$

The dealer secretly sends the shares s_1, s_2, s_3 and s_4 to the participants P_1, P_2, P_3 and P_4 respectively.

If all four participants submit their shares, then the secret S can be recovered as follows:

$$\begin{aligned} S &= s_1 + s_2 + s_3 + s_4 \\ &= 228 + -365 + 98 + 147 \\ &= 108 \end{aligned}$$

Example 2: Let us consider a simple scheme with XOR operations. Let the secrets selected by the dealer be $S = 108$, which is an 8-bit unsigned integer. The dealer further selects three random 8-bit unsigned integers as the first three shares. Let, those are: $s_1 = 228$, $s_2 = 98$ and $s_3 = 186$. The fourth share s_4 can be calculated as:

$$\begin{aligned} s_4 &= S \oplus s_1 \oplus s_2 \oplus s_3 \\ &= 108 \oplus 228 \oplus 98 \oplus 186 \\ &= 80 \end{aligned}$$

The dealer secretly sends the shares s_1, s_2, s_3 and s_4 to the participants P_1, P_2, P_3 and P_4 respectively.

If all four participants submit their shares, then the secret S can be recovered as follows:

$$\begin{aligned} S &= s_1 \oplus s_2 \oplus s_3 \oplus s_4 \\ &= 228 \oplus 98 \oplus 186 \oplus 80 \\ &= 108 \end{aligned}$$

IV. SHAMIR'S TSS SCHEME BASED ON POLYNOMIALS

In this section, we review Shamir's [7] TSS schemes based on Lagrange interpolating polynomial. We also provide an example of Shamir (3, 6)-threshold secret sharing after the scheme is discussed.

Shamir's [7] scheme is based on the following principle: For given t points $\{(x_i, y_i)\}_{i=1}^{t}$ in the 2D plane, we can reconstruct the unique $(t-1)^{\text{th}}$ degree polynomial $f^t(x)$ using Lagrange's interpolation theorem as follows:

$$f^t(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j\neq i}^{t} \frac{(x - x_j)}{(x_i - x_j)} \tag{1}$$

The different phases of the scheme are as follows:

Construction Phase:

Step 1: D chooses a large prime p such that $p > n$ and a secret $S \in \mathbb{Z}_p$.

D generates a $(t-1)^{\text{th}}$ degree polynomial of as follows:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \ (mod\ p) \tag{2}$$

where $a_0 = S$ and $a_1, a_2, \cdots, a_{t-1} \in \mathbb{Z}_p$ are randomly chosen.

Step 2: D computes n unique shares as:

$$s_1 = (1, f(1)), s_2 = (2, f(2)), \cdots, s_n = (n, f(n)) \tag{3}$$

Then he/she sends each s_i to P_i via some secure channels (for $i = 1$ to n).

Recovery Phase:

Without loss of generality, we assume $\{P_i\}_{i=1}^{t}$ submit their shares $\{s_i\}_{i=1}^{t}$. Using Lagrange interpolation, we can find the secret as follows:

$$S = a_0 = f(0) = \sum_{i=1}^{t} f(i) \prod_{j=1, j\neq i}^{t} \frac{-j}{(i-j)} \ (mod\ p) \tag{4}$$

Example 3: Let us consider Shamir (3, 6)-threshold secret sharing.

Construction of Shares: Let the dealer considers $p = 257$ (in practical implementation p has to be a large integer to prevent brute-force attacks) and $S = 108 \in \mathbb{Z}_{257}$.

The dealer assume a 2nd degree polynomial as follows:

$$f(x) = a_0 + a_1 x + a_2 x^2 \ (mod\ p)$$

where $a_0 = S = 108$, $a_1 = 168$, $a_2 = 204 \in \mathbb{Z}_{257}$.

Thus the polynomial is:

$$f(x) = 108 + 168\, x + 204\, x^2 \ (mod\ 257)$$

The shares are generated as

$$\begin{aligned} s_1 &= (1, f(1)) = (1, 223),\\ s_2 &= (2, f(2)) = (2, 232),\\ s_3 &= (3, f(3)) = (3, 135),\\ s_4 &= (4, f(4)) = (4, 189),\\ s_5 &= (5, f(5)) = (5, 137),\\ s_6 &= (6, f(6)) = (6, 136). \end{aligned}$$

The dealer securely transmit each s_i to participant P_i for $i =$ 1 to 6.

Recovery of Secret: Let us consider the participants $P_1, P_2, P_3 \in \mathcal{P}$ submit their shares s_1, s_2, s_3.

$$\begin{aligned} s_1 &= (x_1, f(x_1)) = (1, 223),\\ s_2 &= (x_2, f(x_2)) = (2, 232),\\ s_3 &= (x_3, f(x_3)) = (3, 135), \end{aligned}$$

The secret S can be recovered as follows:

$$\begin{aligned} S = f(0) &= \sum_{i=1}^{3} f(x_i) \prod_{j=1, j\neq i}^{3} \frac{-x_j}{x_i - x_j} \ (mod\ P)\\ &= 223 \cdot (\frac{-x_2}{x_1 - x_2} \cdot \frac{-x_3}{x_1 - x_3}) + 232 \cdot (\frac{-x_1}{x_2 - x_1} \cdot \frac{-x_3}{x_2 - x_3})\\ &\quad + 135 \cdot (\frac{-x_1}{x_3 - x_1} \cdot \frac{-x_2}{x_3 - x_2}) \ (mod\ 257)\\ &= 223 \cdot (\frac{-2}{1 - 2} \cdot \frac{-3}{1 - 3}) + 232 \cdot (\frac{-1}{2 - 1} \cdot \frac{-3}{2 - 3})\\ &\quad + 135 \cdot (\frac{-1}{3 - 1} \cdot \frac{-2}{3 - 2}) \ (mod\ 257)\\ &= 223 \cdot 3 + 232 \cdot -3 + 135 \cdot 1 \ (mod\ 257)\\ &= 108 \end{aligned}$$

Shamir's TSS scheme is a perfect secret sharing scheme, i.e., knowledge of any $t - 1$ or fewer shares is not sufficient to uncover the secret. A large number of secret sharing algorithms are extended from Shamir's SS scheme.

V. SECRET IMAGE SHARING (SIS) SCHEMES

In this section, we present a detailed review of basic SIS schemes. *Visual secret sharing (VSS)* (also known as Visual Cryptography) is the primary SIS scheme. There are some other popular SIS schemes, such as *Polynomial-based SIS, XOR-based SIS, Essential SIS, Scalable and Progressive SIS schemes, SIS schemes with meaningful shares.*

A. VISUAL SECRET SHARING (VSS)

Naor et al. [45] introduced the first visual secret sharing (VSS) or visual cryptography (VC) scheme in 1994. It uses a secure but easy technique that decrypts the secret image from the share images without any cryptographic computation. The secret information can be printed text, handwritten notes, pictures, etc., which are visual and can be encrypted so that the decrypted message also appears as a visual image. The secret message comprises a collection of black and white pixels, where each pixel is considered for encoding. If each share is printed on a separate transparency, then reconstruction can be performed visually by stacking the shares.

Naor and Shamir's VSS Scheme: In the (2, 2) visual secret sharing scheme, every pixel in the original image would be encoded to construct two shares. According to the algorithm, a pixel is expanded by 2 × 2 array of 4 subpixels in each of the two shares. The scheme to substitute a particular pixel with subpixels is shown in Fig. 4. The following two steps show how to select the grid of 4 subpixels (as shown in Fig. 4a) when each pixel of the secret binary image has to be encoded:

Step 1: For a white pixel in the original image, the pixel pairs in the share images are identical, and the selection probability is 0.5 for selecting any one of the corresponding two rows randomly, as shown in Fig. 4b. When these matching grids of the subpixels in two share images overlap, the result becomes a medium gray color, representing white.

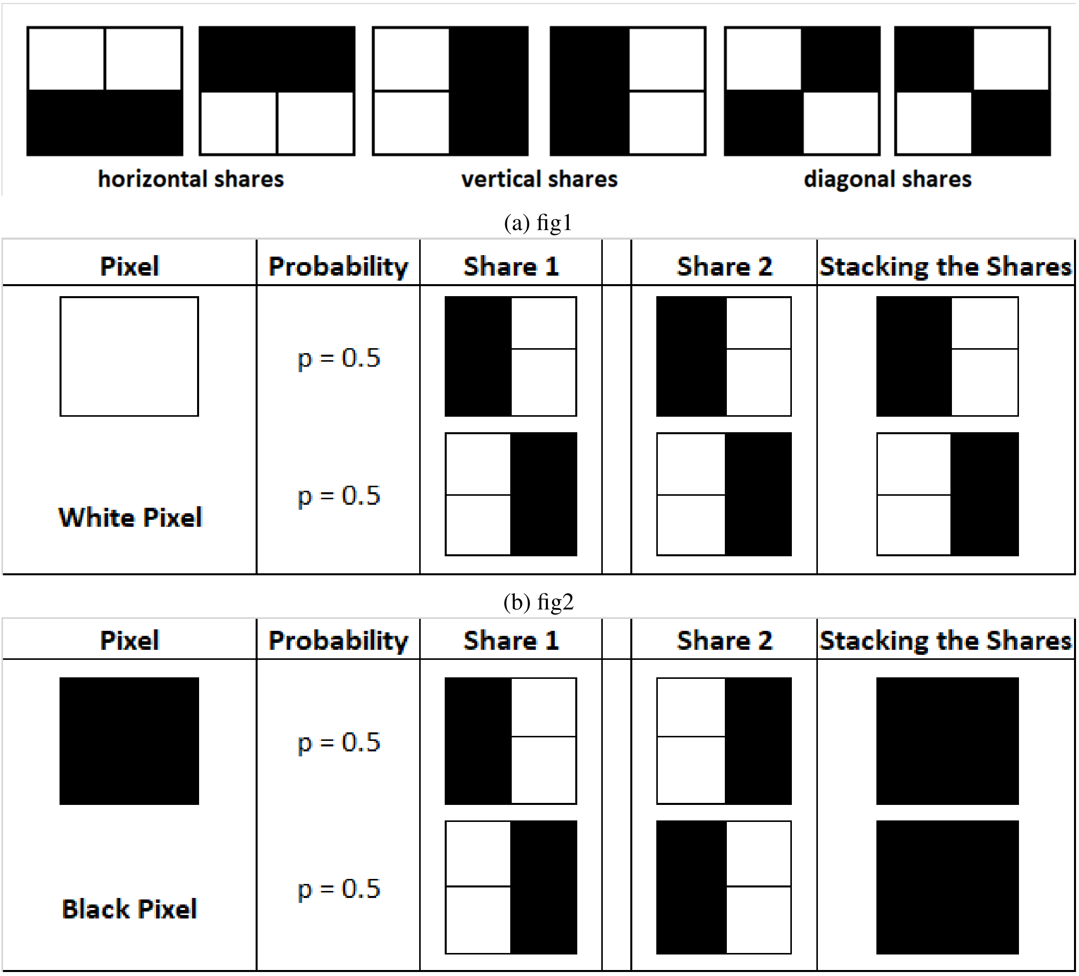
Step 2: For a black pixel in the original image, the pixel pairs in the share images are complementary, and the selection probability is 0.5 for selecting any one of the corresponding two rows randomly, as shown in Fig. 4c. When these complementary grids of the subpixels in two share images are overlapped, the result is black.

The above scheme can be extended to (t, n) threshold VSS scheme. In the (t, n) threshold VSS scheme, there are n distinct transparencies, and if any t or more of them are stacked, the secret image can be regenerated. However, any $t - 1$ shares or fewer than that cannot reveal any information about the secret image. The security parameters in the visual threshold scheme are the same as in the normal threshold scheme. But they are different in the way they reconstruct the secret message. This is a secure technique used in many applications, like banking customer identification or remote electronic voting. However, the above scheme has some limitations. The limitations are mentioned as follows:

- It suffers from the pixel expansion problem that causes each share's size to be four times larger than the original image (as each pixel is expanded by 2 × 2 array of 4 subpixels).
- The recovered image suffers 50% loss of contrast compared to the original image.
- The resulting reconstructed image cannot be stored anywhere, as it has to be recognized visually. Thus, the recovered images are not suitable for further processing. This situation may lead to some real-life problems.

1) VISUAL MULTI-SECRET SHARING (VMSS)

A visual multi-secret sharing (VMSS) scheme was introduced by Wu and Chen [46], where two secret images are concealed into two share images. The prior secret image can be recovered if two share images are stacked together. The later secret image can be recovered if the first share is rotated by 90° anticlockwise. The major limitations of this scheme



(a) fig1

(b) fig2

(c) fig3

FIGURE 4. Subpixels selection in Naor and Shamir's Scheme.

are that it can be applied to exactly two secret images, and the natural rotating angle can be 90°, 180° or 270° such that the secret images retain their rectangular shape. Katoh and Imai [47] proposed a scheme for visual multi-secret image sharing where a new secret is reconstructed every time a new layer is stacked over the previous one. Later, Wu and Chang [48] invented a scheme where the shares are circular instead of rectangular. This scheme encodes two secret images without the angle's limitation, compared to Wu and Chen's [46] scheme. Hsu et al. [49] proposed another scheme to overcome the angle constraint in Wu and Chen's [46] scheme. In their scheme, two sets of secret images can be encoded in two ring-shaped share images, and good-quality secret images are revealed by rotation of the share images at any arbitrary angle around the entire 360° ring. In order to encode more secrets, Shyu et al. [50] proposed another scheme that conceals k ($k \geq 2$) secret images into two circular shares. All the k secret images can be obtained by staking the first share and rotating the second share at different angles. However, the shapes of the recovered images are distorted from square to circular, and the recovered images have poor contrast. Fu and Yu [51] proposed a scheme where four secret images are encoded into two share images, and the secrets can be recovered by stacking the two shares with distinct angles without shape distortions. Chen et al. [52] developed a MSIS scheme without pixel expansion, where two secret images are encoded into meaningless random grids without using a codebook. During decryption, the first secret image is reconstructed by stacking two random grids on top of each other. They invented a unique technique to rotate the random grids used to recover the second secret image. Four secret images are embedded into two shares using Shyu's [53] random-grid-based VSS scheme. Chen et al. [52] proposed another random-grid-based VSS scheme, which can also embed four secret images into two shares without pixel expansion. All the secrets can be revealed by stacking the shares and rotating one of the two shares at 0°, 90°, 180°, and 270° respectively. The limitation of these schemes is that the share images generated are meaningless (random-like shares), and attackers suspect those as encrypted images and consider them subjects of different cryptographic attacks.

All the VSS schemes we discussed above generate the share images as meaningless, noise-like images. Attackers can easily suspect them as encrypted images and attempt to execute several analyses. Liu et al. [54] proposed a black-and-white $(2, 2)$- VMSS scheme for encoding three secret images into two share images without pixel expansion. The main advantage of their scheme is that they have created meaningful share images using a camouflaging algorithm so that attackers cannot recognize them as share images. Chen et al. [55] introduced a new VSS scheme using a fixed-angle segmentation technique to create circular share images. Two or more circular-shaped shares can be stacked at all different 360 stacking angles to reveal the secrets. Yang and Chen [56] proposed a scheme with high-quality share images based on the gray and white subpixels. They have replaced gray subpixels with black subpixels in the share images in their scheme. Chen et al. [57] proposed a VMSS scheme using many weighted transparencies where qualified subsets are stacked to reveal a secret at each stacking level. The transparency with a comparatively larger weight decides which secret image will be reconstructed. Feng et al. [58] introduced a different variant of the VMSS technique, which allows any number of independent secret images to be encoded within two sharing images. These encoded images may then be decrypted using aliquot stacking angles. Shyu and Chen [59] created a visual cryptographic method that is capable of encoding two or four secret images into two rectangular shares. Reconstructing the secret images requires a series of processes that involve flipping operations. Mishra and Gupta [60] proposed a $(2, n, m)$ VMSS scheme using an iterative method, where n shares are generated to encode m secret images. The advantage of this scheme is, it is used for m secret images where $m \geq 2$. If the shares from a qualified set are pooled together, the secret images are revealed. If the shares are taken from the forbidden set, however, none of the information concerning the secrets will be disclosed. To obtain one secret image, a minimum of two shares are used, and to obtain m multi-secret images, n or $m + 1$ shares are required. The scheme does not require the shares to be perfectly aligned in order to obtain the secret images. This technique is based on the stacking of shares and adheres to the concept of VC. Previous methods were restricted to a fixed number of secret images with a minimum number of shares, and the correct alignment of shares was necessary to obtain the secret images. Mishra and Gupta's [60] scheme solved the limitations of the previous algorithms and provided security to multiple images in an efficient way.

2) VSS COLOR IMAGE

Naor and Shamir [61] introduced the formal study of Visual Cryptography in the field of color images. They also proposed a $(2, n)$-VC scheme for color images containing two transparent colors. Rijmen [62] proposed a $(2, 2)$-VC scheme based on the concept of color mixture. The idea behind the scheme is that each pixel is divided into m subpixels of m distinct colors, and stacking such two pixels results in the third color. With the stacking of two pixels with different permutations of subpixels, we can produce $n!$ number of different colors. In the basic version of the scheme, each pixel is divided into four subpixels, having the colors red, green, blue, and white. Hence, by staking such two pixels $4! = 24$ colors can be generated. However, Yang [63] have corrected the claim and shown that actually $4! - 7 = 17$ unique colors can be generated. Hou [64] applied halftone technology and the color decomposition method to propose three different $(2, 2)$-VC schemes for color images. Using color decomposition, the secret image is decomposed into cyan, magenta, and yellow halftone images. Then, by utilizing a few existing binary VC schemes, the different VC schemes for color images are implemented.

The VC schemes for color images we have discussed so far are either $(2, 2)$ or $(2, n)$ in nature. Verheul and Van Tilborg [65] introduced two VC schemes for c-colored images (c is the number of distinct colors used in secret images) with a general (t, n)-threshold structure. The pixel expansion observed in this scheme is q^{t-1} where $q \geq c$. Further, Koga and Yamamoto [66] proposed another (t, n)-VC scheme for c-colored images based of finite lattice structure. In another (n, n)-scheme, they have reduced the pixel expansion to $c \times 2^{n-1}$ for a secret c-colored image. Yang and Laih [67] proposed a (t, n)-VSS scheme based on a few existing (t, n)-binary VSS schemes with the pixel expansion $m \times c$, where m is the pixel expansion in the basis binary VSS scheme. Blundo et al. [68] presented various constructions of $(2, n)$, (t, n) and (n, n) VSS schemes. In their (n, n) VSS scheme, the pixel expansion is measured as $(c-1)2^{n-1}-c+2$, if n is odd; and $(c - 1)2^{n-1} - c$, if n is even. Chen and Tsao [69] first proposed a VSS scheme based on random grids that produces meaningful shares. The authors used the cover image for generating meaningful shares and solving the problem of pixel expansion. Chen and Tsao [70] proposed another (t, n) threshold VSS scheme using random grids for binary and color images. Yan et al. [71] proposed a VSS scheme based on random grids that also produces meaningful shares. This scheme can reconstruct the original image with better visual quality than the scheme proposed by Chen and Tsao [70]. Another scheme proposed by Yan et al. [72] is also a threshold VSS with OR and XOR decryption abilities. Yan et al. [73], later, proposed one more (t, n) threshold VSS scheme based on random grids with better quality of the reconstructed image visually.

Adhikari [74] presented a $(2, n)$ VSS scheme for color images. They established a minimum color ratio for the scheme. This lower bound on the color ratio is not dependent on the number of shares but rather on the number of colors in the secret image. Therefore, the scheme achieves a better color ratio, and the resultant images are brighter than the result achieved by Koga and Yamamoto [66]. Cimato et al. [75] presented a detailed study of c-color

(t, n)-threshold VSS schemes and reported characterization on contrast-optimal schemes. Cimato et al. identified a special class of schemes, referred to as canonical schemes, that satisfy the strong symmetry property. They used canonical schemes to provide constructive proof of optimality for (n, n) VSS schemes with respect to pixel expansion. They also provided constructions of c-color $(2, n)$-threshold schemes with improved pixel expansion compared to most of the previously proposed schemes for color images. The pixel expansion for the (n, n) VSS scheme is $c \times 2^{n-1} - 1$, if n is even, and $c \times 2^{n-1} - c + 1$, if n is odd. Chen and Wu [76] presented another efficient c-color (t, n) VSS scheme having pixel expansion measured as $\lceil log_2 n \rceil \times m$ (where m is the pixel expansion of the existing binary (t, n)-VSS scheme used for its implementation). The scheme is superior in comparison to the schemes by Yang and Laih [67], and Blundo et al. [68], when c, the number of colors in the secret image becomes large. Cimato et al. [77] presented a colored visual cryptographic model that ensures the reconstruction of every secret pixel with its original color, rather than becoming a darker version of the original one like most of the previous schemes. The pixel expansion of the resulting c-color VSS scheme is $c\binom{n}{k}2^{k-2}$ and it achieves maximal contrast in comparison with the previous schemes. They also developed another c-color $(2, n)$-threshold scheme with pixel expansion $c(n - 1)$. Shyu and Chen [78] proposed a (t, n) VSS scheme that further reduces the pixel expansion by using a simple and effective integer linear program. Adhikari [74] reported a construction method for a robust monochrome VSS scheme with a general access structure using linear algebra. Furthermore, the author presented various VSS schemes with the (t, n) and (n, n)-threshold structures. The main benefit of this (n, n) VSS scheme is that it attains optimal pixel expansion and optimal relative contrast. The author also extended the monochrome VSS scheme to the colored VSS scheme for restricted access structures.

The Boolean-based VC schemes use either bitwise OR or bitwise XOR operations. If OR-based VC Schemes are compared with XOR-based VC Schemes, it can be observed that XOR-based VC schemes are able to generate better relative contrast in the recovered secret images. Further, it is possible to achieve relative contrast $=$ 1 in case of some XOR-based VC schemes, which is impossible in the case of OR-based VC schemes. Dutta and Adhikari [79] presented a comprehensive theoretical study to determine a necessary and sufficient condition for an XOR-based visual cryptographic scheme to attain optimal relative contrast equal to 1 in terms of access structure. They have used combinatorial design cumulative array to show that with XOR-based VC, relative contrast 1 can be achieved if and only if the given access structure is optimal (the criteria for optimality of access structure are detailed in [79]). Dutta et al. [80] proposed a theoretic c-color VC scheme realizing general access structure, where construction achieves maximal contrast. Moreover, they have presented an efficient (t, n)-threshold VC scheme for color images. Their construction method is superior to the existing schemes in terms of pixel expansion.

3) PROBABILISTIC VSS

Security, accuracy, rate of pixel expansion, and computational complexity are the basic criteria used to evaluate the performance of a (t, n) VSS scheme. Many (t, n) VSS schemes [65], [67], [81], [82], [83] satisfy the security and accuracy criteria, whereas VSS schemes such as [82] and [83] suffer from the pixel expansion problem. Later, the VSS schemes [84], [85] solved the pixel expansion problem, although those schemes suffer from high computational complexity. A special type of VSS scheme known as the probabilistic visual secret sharing (ProbVSS) scheme proposed by Yang [86] provides solutions for the computation complexity problem and the pixel expansion problem. However, the reconstruction accuracy capacity decreased slightly. Cimato et al. [87] proposed another ProbVSS scheme, applicable for binary images. Later, Wang et al. [88] proposed a probabilistic $(2, n)$ visual secret sharing scheme, or $(2, n)$ ProbVSS scheme, for binary images and a deterministic (n, n) secret image sharing scheme for grayscale images. Although both schemes solve the issues of computational complexity and pixel expansion, there are still some limitations. The scheme cannot be applied to color images. Chang et al. [89] combined Shamir's [7] scheme and Chang and Wu's gradual search algorithm for a single bitmap BTC (GSBTC) [90] and proposed a new $(2, n)$ ProbVSS scheme, based on Wang et al.'s $(2, n)$ ProbVSS scheme. The main advantage of Chang et al.'s [89] scheme is that it can be applied to color images. Also, the reconstructed color images generated by the scheme are of high quality, and shadow size is also reduced without significantly increasing computational complexity. The other limitation of Wang et al.'s [88] scheme, as reported by Chang et al. [91] is that the quality of the reconstructed image is decreased when the $(2, n)$ ProbVSS scheme is repeated eight times to deal with grayscale images and any two of n shadows are used to reconstruct the grayscale image. Chang et al. [91] applied two strategies to Wang et al.'s scheme: the voting strategy and the least significant bits abandoning approach, and proposed a modified scheme in combination with Wang et al.'s $(2, n)$ ProbVSS for binary images to handle grayscale images. The PSNR of the reconstructed image in Chang et al.'s [91] scheme is greater by about 1 dB than that in Wang et al.'s [88] scheme. Also, the computational complexity is lower in comparison with Wang et al.'s scheme. Later, to reduce the pixel expansion significantly while maintaining acceptable visual quality, De Prisco and De Santis [94] proposed a new model for VC schemes called color-black-and-white VCS (CBW-VCS). In CBW-VC schemes, each binary pixel from the secret image is encoded into several shared color pixels, and in this approach, the pixel expansion can be reduced considerably. Recently, Wu and Yang [95] presented two constructions for a (t, n)-threshold probabilistic CBW-VC scheme. Both construction methods generate color shares

TABLE 3. Comparison between a few VSS schemes.

Schemes	Type of scheme	Secret image type	Pixel expansion	Share type	Multi-secret sharing	Access structure	Verifiable
Naor-Shamir [45]	VSS	binary	yes	meaningless	no	$(2,2)$, (t,n)	no
Yang and Laih [67]	VSS	colored	yes	meaningless	no	(t,n)	no
Lin and Tsai [19]	VSS	grayscale	yes	meaningless	no	(t,n)	no
Wang et al. [88] scheme-1	ProbVSS	binary	no	meaningless	no	$(2,n)$	no
Shyu et al. [53]	VSS	binary/grayscale/colored	no	meaningless	no	$(2,2)$	no
Chen and Tsao [70]	VSS	binary/colored	no	meaningless	no	(t,n)	no
Chen and Tsao [69]	VSS	binary/grayscale/colored	no	meaningful	no	$(2,2)$	no
Chen et al. [92]	VSS	binary/grayscale/colored	yes	meaningless	no	$(2,n)$	yes
Ou et al. [93]	VSS	binary/grayscale/colored	no	meaningful	no	(n,n)	no
Yan et al. [71]	VSS	binary	no	meaningful	no	(t,n)	no
Yan et al. [72]	VMSS	binary	no	meaningless	yes	(t,n)	no
Liu et al. [54]	VMSS	binary	no	meaningful	yes	$(2,2)$	yes
Lin et al. [30]	VMSS	binary	yes	meaningful	yes	(t,n)	yes
Yan et al. [73]	VSS	binary	no	meaningless	no	(t,n)	no
Mishra and Gupta [60]	VMSS	binary	no	meaningless	yes	$(2,n,m)$	yes
Dutta et al. [80]	VSS	colored	yes	meaningless	no	(t,n)	no
De Prisco and De Santis [94]	ProbVSS	binary/grayscale/colored	yes	meaningless	no	(t,n)	no
Wu and Yang [95]	ProbVSS	binary/grayscale/colored	no	meaningless	no	(t,n)	no

without pixel expansion problem. We compared a few VSS, VMSS, and ProbVSS schemes in table 3.

B. POLYNOMIAL-BASED SECRET IMAGE SHARING

The polynomial-based SIS (PSIS) schemes are based on Shamir's [7] TSS scheme. Although Shamir's scheme can also be used for secret image sharing, considering each pixel as a secret, due to the large size of images, it results in a huge number of shares. It causes a waste of memory and communication bandwidth. This motivated researchers to develop polynomial-based methods that generate share images smaller than the secret image. Thien and Lin [14] presented a (t, n)-threshold SIS scheme (Thien-Lin scheme), which can generate share images, having the size $\frac{1}{t}$ of the secret image size. However, the reconstruction of the secret image is lossy, and the recovered secret image can be slightly distorted. Thien and Lin also proposed a lossless version of the scheme with a slight increase in share sizes (as the size becomes $\frac{1}{t-1}$ times of the secret size). The Thien-Lin scheme requires a considerable amount of computation for an initial permutation to reduce the strong correlation between adjacent pixels in the secret image.

1) THIEN-LIN SCHEME

In Thien-Lin [14] scheme, the secret image taken is a grayscale image. Let the secret image be I_s. As the gray value of a pixel lies between 0 and 255, the prime p for the polynomial $g(x)$ mod p is considered 251, which is the greatest prime in the given interval. All the operations are performed in the prime Galois Field $GF(251)$. Hence, preprocessing is necessary to truncate pixel values larger than 250.

Construction Phase: The dealer D perform the following steps to generate the shares:

Step 1: Truncate all the gray values greater than 250 to 250, such that the range of pixel values in I_s is 0-250.

Step 2: Choose a key to generate a permutation sequence to permute the pixels of the secret image I_s. Let the permuted image be I'_s.

Step 3: Set the section number j to 1.

Step 4: Generate a new section j by considering t pixels, which are yet-not-processed in a continuous manner from the permuted secret image I'_s.

Step 5: For section j, generate a $(t-1)^{\text{th}}$ degree polynomial $g_j(x)$ as follows:

$$g_j(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1} \; mod \; 251 \quad (5)$$

where $\{a_i\}_{i=0}^{t-1}$ are the consecutive t pixels from the section j. Also evaluate $g_j(1), g_j(2), \cdots, g_j(n)$.

Step 6: Increase j by 1.

Step 7: Repeat steps 4-5 until all pixels of I'_s are processed.

Step 8: Arrange the n pixels $\{g_j(i)\}_{i=1}^{n}$ from section j into n share images $\{SI_i\}_{i=1}^{n}$ in a sequential manner, such that share image SI_i contains $g_j(i)$ for all sections j sequentially. It is obvious that the size of each share image becomes $\frac{1}{t}$ of the secret image.

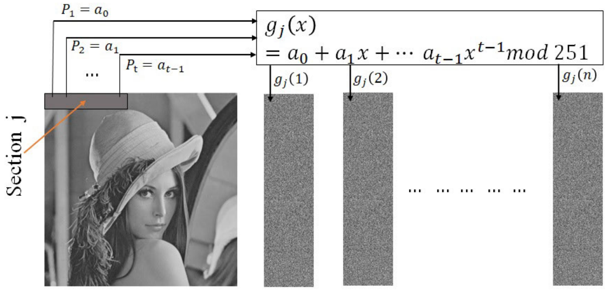


FIGURE 5. Thien-Lin scheme.

Step 9: Distribute n share images $\{SI_i\}_{i=1}^{n}$, and the permutation key must be sent secretly.

Recovery Phase: The combiner C performs the steps below to reveal the secret image from t or more ($\leq$ n) share images. Without loss of generality, let t share images are $\{SI_i\}_{i=1}^{t}$.

Step 1: Set the current processing section j to 1.

Step 2: Consider the first non-processed pixels from each of the t share images SI_i for $i = 1, 2, \cdots, t$.

Step 3: Given t pixel values, which are $\{g_j(1), g_j(2), \cdots, g_j(t)\}$, Lagrange's interpolation used to determine the unique polynomial. The recovered coefficients $\{a_0, a_1, \cdots, a_{(t-1)}\}$ are nothing but the consecutive t pixel values of the I'_s.

Step 4: Increment j by 1.

Step 5: Repeat the step 2-4 until all the pixels of t share images are processed. At the end of this step, the permuted secret images I'_s can be recovered.

Step 6: Using the key, regenerate the permutation sequence, and perform inverse-permutation on I'_s to reveal the secret image I_s. Fig. 5 depicts the concept of Thien-Lin Scheme [14].

Instead of manipulating the secret image in the spatial domain, Lin et al. [96] used the discrete cosine transform (DCT) to transform the secret image into the frequency domain, which drastically reduced the amount of data to be shared. The scheme is applicable for color images and can be easily extended for compression standards like JPEG, MPEG, etc. Chang et al. [97] have combined a gradual search algorithm for a single bitmap BTC (block truncation coding) or GSBTC (proposed by [90] Chang and Wu) with Shamir's polynomial-based SS and proposed a new scheme to share color images. Both the schemes [96], [97] can guarantee the recovered image's satisfactory quality.

Wang and Su [98] and Wu [99] proposed a lossless version of Thien-Lin scheme. To avoid the loss of information, Wang and Su [98] proposed all the calculations in $GF(2^k)$ (where k-bit secret image is considered) instead of $GF(p)$ (where $p = 251$ in Thien-Lin scheme). They have further reduced the share image size, which is about 40% smaller than the Thien-Lin scheme using Huffman encoding and image differencing process. The scheme performs lossless recovery without compromising the size of share images. The authors presented a modified version of their proposed scheme, which reduces the probability of error propagation. The Huffman encoding and image differencing process initially performed on the secret image significantly reduced the strong correlation between the neighboring pixels in the secret image. As a result, the initial permutation in Thien-Lin scheme is no longer required. However, the preprocessing still incurs substantial computation costs. Wu [99] used the prime for modulo operations as 257 instead of 251 (as specified by Thien-Lin scheme). This process resolves the overflow problem in the Thien-Lin scheme; however, pixel values of 0 are affected. To solve this problem, Wu has proposed a special decoding technique. Further, Kanso and Ghebleh [100] proposed another polynomial-based SIS scheme that applies a circular right shift for each pixel value to modify only the least significant bit of the targeted pixel value. It makes less intrusive changes to the secret image compared to the Thien-Lin scheme.

For Thien-Lin's [14] scheme and many of its derivative schemes, the preprocessing of the secret image is based on permutation. Jolfaei and Wu [101] conducted a detailed study on cryptanalysis of permutation-only cipher images and proved the permutation-only image ciphers are easily at risk to a chosen-plaintext attack. Further, Zhou et al. [102] have shown that Thien-Lin's (t, n)-threshold scheme [14], and many of its extensions are not secure, as with $(t - 1)$ share images, it is possible to reveal partial information about the secret image. To overcome this problem, they have proposed to encrypt the pixels of the secret image as part of preprocessing. In their proposed scheme, the share images generated are slightly larger than Thein-Lin scheme, and the preprocessing of pixels involves a considerable computation cost. In another polynomial-based SIS scheme [103], Ghebleh and Kanso considered the secret image an array of b-byte integers. The b and the large prime p must be chosen such that p is the largest prime less than 2^{8b}, and $t \leq n < p$. Their scheme accommodated a sizeable finite field, and they grouped multiple bytes (pixels) into single values, which makes it less intrusive than most of the previous schemes [14], [100]. The use of a very large finite field $GF(p)$ (where p is a large prime such that for grayscale images $2^8 \leq p \leq 2^{8b}$, and for color images $2^{24} \leq p \leq 2^{24b}$) improves the quality of the recovered images. However, it involves high costs in the reconstruction process. Ghebleh and Kanso have also proposed a lossless version of their SIS scheme. Azzahra and Sugeng [104] introduced a reliable (t, n) SIS scheme using matrix projection for sharing and verifiability. Sardar and Adhikari [105] proposed another SIS scheme for RGB color images, which does not require any preprocessing at all; besides, it is able to reconstruct the exact secret image in a lossless way.

Many SIS schemes are developed based on the Chinese remainder theorem (CRT). Meher and Patra [106] proposed a primitive SIS scheme based on CRT to share a single image. However, the scheme cannot ensure threshold security criteria. Based on CRT, Shyu and Chen [107] presented a (t, n)-threshold SIS scheme. Chang et al. [108] combined Lagrange interpolation and CRT to present another (t, n)-threshold MSIS scheme, which can recover all the secret images in a lossless way. We compared a few polynomial-based SIS schemes in Table 4.

C. XOR-BASED SECRET IMAGE SHARING

Wang et al. [88] presented two SIS schemes. First, they proposed a $(2, n)$ ProbVSS scheme for binary images, which is dependent on XOR and AND operations. The authors have shown that the construct of the recovered images is better than previous probabilistic schemes and does not suffer from the pixel expansion problem. Afterward, they proposed a deterministic (n, n) SIS scheme (where $n \geq 2$) for grayscale images based on XOR operations, where the regeneration of the original secret image is entirely lossless. In the following subsection, we briefly describe the XOR-based (n, n) SIS scheme presented by Wang et al. [88].

1) WANG-ZHANG-MA-LI'S SCHEME [88]

Consider the grayscale secret image I_s, which is of size $w \times h$.

Construction Phase:

Step 1: The dealer D makes $n - 1$ random matrices $\{B_1, B_2, \cdots, B_{n-1}\}$ of size $w \times h$ such that each value is from the range [0-255].

Step 2: D computes the n share images $\{SI_1, SI_2, \cdots, SI_n\}$ as follows:

$$\begin{aligned} SI_1 &= B_1, \\ SI_2 &= B_1 \oplus B_2, \\ &\cdots, \\ SI_{n-1} &= B_{n-2} \oplus B_{n-1}, \\ SI_n &= B_{n-1} \oplus I_s, \end{aligned} \tag{6}$$

Recovery Phase

The combiner can reveal the secret as follows:

$$I'_s = SI_1 \oplus SI_2 \oplus \cdots \oplus SI_n. \tag{7}$$

Although the scheme is defined for grayscale images, it can also be applied to binary images and color images.

The XOR-based SIS scheme by Wang et al. has several advantages compared to the traditional VC schemes: (1) the recovery of the secret image is completely lossless; (2) the secret image can be either binary, grayscale, or color; (3) the pixel expansion problem no longer exists; (4) the recovered image has perfect contrast; (5) there is no alignment problem: the challenge of correctly aligning the share images to reveal the secret image; and (6) there is no requirement of the codebook. More importantly, all these advantages are available with a low computation cost (less than any polynomial based SIS scheme), as all the operations are XOR-operations. However, the size of share images is the same as the size of secret images, resulting in deficient sharing capability (sharing capability is defined as the ratio of the number of secret images to the number of share images). Chen and Wu [76] presented an (n, n) MSIS scheme to share $n - 1$ secret images. Hence, it provides a sharing capacity

TABLE 4. Comparison between a few polynomial-based SIS schemes.

Schemes	Secret image type	Pixel expansion	Lossless recovery	Share size	Share type	Multi-secret sharing	Access structure	Verifiable
Thien-Lin [14] scheme-1	grayscale	no	no	$\frac{1}{t}$	meaningless	no	(t, n)	no
Thien-Lin [14] scheme-2	grayscale	no	yes	$\geq \frac{1}{t}$	meaningless	no	(t, n)	no
Wang and Su [98]	grayscale	no	yes	$\frac{1}{t}$	meaningless	no	(t, n)	no
Wu [99]	grayscale	no	yes	$\frac{1}{t}$	meaningless	no	(t, n)	no
Zhao et al. [109] scheme-1	grayscale	no	no	$\frac{1}{t}$	meaningless	no	(t, n)	yes
Zhao et al. [109] scheme-2	grayscale	no	yes	$\geq \frac{1}{t}$	meaningless	no	(t, n)	yes
Chang et al. [108]	binary/grayscale/colored	yes	yes	1	meaningless	yes	(t, n)	no
Kanso-Ghebleh [100]	grayscale/colored	no	no	$\frac{1}{t}$	meaningless	no	(t, n)	no
Liu et al. [31]	grayscale	no	no	$\frac{1}{t-1}$	meaningless	yes	(t, n)	yes
Azzahra et al. [104]	grayscale	no	no	$\frac{1}{t} + \frac{1}{m}$	meaningless	yes	(t, n)	yes
Zhou et al. [102]	grayscale	no	no	$\frac{1}{t}$	meaningless	no	(t, n)	no
Ghebleh-Kanso [103] scheme-1	grayscale/colored	no	no	$\frac{1}{t-1}$	meaningless	no	(t, n)	no
Ghebleh-Kanso [103] scheme-2	grayscale/colored	no	yes	$\frac{t-1}{b} + \frac{1}{k-1}$	meaningless	no	(t, n)	no
Ma et al. [110]	grayscale/colored	no	yes	$\frac{2}{(2t-1)}$	meaningless	no	(t, n)	yes
Sardar-Adhikari [105]	colored	no	yes	$\frac{1}{t-1}$	meaningless	no	(t, n)	no

TABLE 5. Comparison between a few XOR-based SIS schemes.

Schemes	Secret image type	Lossless recovery	Share size	Share type	Multi-secret sharing	Access structure	Verifiable
Wang et al. [88] scheme-2	binary/grayscale/colored	yes	1	meaningless	no	(n, n)	no
Chen-Wu [76]	binary/grayscale/colored	yes	1	meaningless	yes	(n, n)	no
Chen-Wu [22]	binary/grayscale/colored	yes	1	meaningless	yes	(n, n)	no
Ou et al. [117]	binary	yes	$\frac{1}{4}$	meaningful	no	(n, n)	yes
Chen et al. [112]	binary/grayscale/colored	yes	1	meaningless	yes	(n, n)	no
Guo et al. [113]	binary	yes	1	meaningful	yes	(t, n)	no
Faraoun [114]	binary/grayscale/colored	yes	1	meaningless	yes	(n, n)	no
Deshmukh et al. [24]	colored	yes	1	meaningful	no	(n, n)	no
Chattopadhyay et al. [32]	binary/grayscale/colored	yes	1	meaningless	yes	(n, n)	no
Kabirirad and Eslami [118]	colored	yes	1	meaningful	no	(t, n)	no
Prasetyo-Hsia [119]	binary/grayscale/colored	conditional	1	meaningless	no	(n, n)-progressive	no
Nag et al. [120]	grayscale/colored	yes	1	meaningless	yes	access-structure-based	no
Chattopadhyay et al. [121]	binary/grayscale/colored	yes	1	meaningless	yes	(n, n)	yes
Chattopadhyay et al. [122]	binary/grayscale/colored	yes	1	meaningless	yes	(t, n)	yes
Soreng and kandar [33]	binary/grayscale	yes	1	meaningless	yes	(t, n)	yes

of $\frac{n-1}{n}$, which is far better than one proposed by Wang et al. [88]. Chen and Wu [22] identified a major drawback in [76]: the share images are not completely randomized, hence not very secure. Chen and Wu [22] proposed another (n, n) MSIS scheme using a random image generator function and XOR operations to share n secret images through n share images. Chen and Wu's [22] scheme constructs randomized share images and has better sharing capability than [76]. However, Yang et al. [111] showed that the (n, n) MSIS [22] does not satisfy the threshold security criteria, as one can reveal partial information about the secret images with $n-1$ or fewer shares. They have removed this limitation and proposed a strong threshold (n, n) MSIS scheme, which guarantees that without having n number of shares, no secret image related information can be revealed. Chen et al. [112] proposed a symmetric sharing-recovery function (SSRF) based on XOR operations and other Boolean operations. Using this SSRF, they have presented an (n, n) MSIS scheme that can share n secret images. In comparison to the schemes in [22] and [76], the scheme [112] has a low level of computing complexity and a high level of security. Both schemes [22], [76] use randomly generated images to randomize the secret images, and the randomized form of the secret images is utilized to generate the share images. However, the pseudorandom number generator (PRNG) functions applied to generate the random images may have poor security attributes, like short periods and predictable sequences. As a consequence of this, share images are vulnerable to assaults using statistical cryptanalysis. Guo et al. [113] presented a MSIS scheme along with a general access structure. The authors combined the CRT method with XOR operations to construct meaningful share images. Faraoun [114] presented a highly secure (n, n) MSIS scheme based on a cryptographic hash function and a secure stream cipher. Further, Chen and Chen [115] extended the MSIS scheme by Chen et al. [112] and came up with two new schemes: a partial sensitivity different-sized symmetric sharing-recovery (PDSR) scheme and a full sensitivity different-sized symmetric sharing-recovery (FDSR) scheme. Both schemes can share secret images of different sizes and use the same function for the sharing and recovery processes. Nevertheless, these two schemes show a different degree of sensitivity when share images are under attack. Any attack on share images in the PDSR scheme fails to disclose any secret images. For the FDSR scheme, however, two terms are introduced: *minimum-sized area* refers to the area under the minimum horizontal index and minimum vertical index between the secret images, and *maximum-sized area* refers to the area under the maximum horizontal index and maximum vertical index between the secret images. Any attack outside the minimum-sized area of shared shares fails to disclose the attack area of the corresponding secret image under the FDSR scheme. Kabirirad and Eslami [116] proved that the (n, n) MSIS scheme in [112], and two MSIS schemes in [115] do not fulfill the threshold security criteria. In all three schemes, one with $n-1$ or fewer shares can disclose partial data about secret images with efficient computation. They have also addressed the security issue with some extra Boolean operations.

Deshmukh et al. [24] presented an (n, n) MSIS scheme based on CRT and XOR operations. Although this scheme ensures higher security and randomness than most of the XOR-based MSIS schemes, it involves a high computation cost. The time complexity of the scheme is dependent upon a variety of criteria, including the bit depth, the number of shares, and the size of the secret image. Another three different schemes are presented by Deshmukh et al. [123]; among them, the first two schemes are based on XOR operations, and the third one is based on arithmetic modulo operations. They have experimentally shown that the MSIS scheme implemented using modular arithmetic requires less computation than the XOR-based MSIS schemes. Prasetyo and Guo [23] detected a limitation in the scheme presented in [24], that the scheme fails to reconstruct secret images correctly if the number of secret images considered for sharing is odd. They have proposed an improved MSIS scheme to solve this problem. They have also proposed a method of sharing by using hyperchaotic image scrambling, which ensures a high level of security for the MSIS scheme. Another MSIS with a general access structure is presented by Nag et al. [120]. Prasetyo and Hsia [119] presented two progressive SIS schemes. Their first scheme is based on the generalized random grid, and the second one is based on XOR operations. Both of the progressive SIS schemes fulfill the lossless recovery criteria. Chattopadhyay et al. [32] proposed a XOR based (n, n) VSIS scheme, which can generate smaller share images. Chattopadhyay et al. [121] presented another verifiable (n, n) MSIS scheme based on XOR operations, a secure hash function, and a pseudo-random image matrix generator function. All the XOR-based schemes so far discussed have (n, n) threshold structure. Kabirirad and Eslami [118] proposed a more general (t, n)-threshold structure for their MSIS scheme with XOR operations. However, the scheme has a restriction on the consecutiveness of shares, that is, all the t shares must be in a specified order. Several merits of using XOR-based schemes are: (1) lossless reconstruction; (2) no pixel expansion; (3) perfect contrast in the recovered images; and (4) very low computation involved. However, the disadvantages are: (1) the share size and secret size are the same, and (2) most of the schemes use (n, n)-threshold structure. Later, Chattopadhyay et al. [122] presented one more efficient verifiable (t, n) SIS scheme based on XOR operations. The verifiability and security of the scheme were achieved using elliptic curve cryptography (ECC). We compared a few XOR-based SIS schemes in Table 5.

D. ESSENTIAL SECRET IMAGE SHARING (ESIS)

Each participant has the same priority in a conventional (t, n) SIS scheme. However, in some practical scenarios, a few participants may have more priority than the rest based on their importance. Hence, the shares can have different priorities in the reconstruction process. Weighted secret image sharing (WSIS) generates shadows with different priorities or weights depending on the participants' importance. The secret image can be revealed if the weight of the submitted share images is at least t_w, which is the threshold weight. Chen et al. [124] introduced a weighted secret sharing method having two main components: (1) a histogram modulation and (2) a two-layer structure. In a two-layer structure, they have divided the participants into several groups depending on their importance in revealing the secret, then different groups assigned with different weights. However, in this scheme, a shadow with larger weight cannot replace a shadow with a smaller weight. Thus, it cannot be considered a proper WSIS scheme. Shyu et al. [125] proposed a WSIS scheme based on the Chinese remainder theorem (CRT), in which the dealer can distribute share images of various sizes and able to assign a distinct weight for each share. Instead of depending on the overall weight of the shadows, the recovery of the secret is dependent on the number of shadows that are provided. An appropriate implementation of WSIS can be observed in the scheme proposed by Lin et al. [126]. Lin et al. proposed a practical polynomial-based WSIS, where the dealer is able to create shadows of various sizes based on their respective weights. The secret image can only be retrieved if the combined weight of all submitted shadows is higher or equal to the threshold weight. Although WSIS schemes solve the problem of assigning distinct priorities to participants in practical scenarios, it becomes almost impossible to assign separate weightage to the participants according to their importance to reveal the secrets.

A simple and effective solution to this issue is to split the participants into two separate groups: an essential group with higher priority than that of another group called a non-essential group. In the reconstruction process, submission of a threshold or more number is necessary, but not sufficient. The submission from at least a threshold number of essential participants is also a must. These essential SIS (ESIS) schemes are simple and more practical than WSIS schemes. In 2013, Li et al. [127] introduced a general (t, s, k, n)-essential SIS scheme. The basic principle of their scheme is n shadows are divided into s essential shadows and $(n - s)$ non-essential shadows, and to reconstruct the secret image, k shadows are required, which should include at least t essential shadows. Yang et al. [21] proposed another (t, s, k, n)-ESIS scheme, where they have reduced the size of total shadows by using the two-layered conjunctive hierarchical approach. Also, in this scheme, the size of required share images in reconstruction is less than Li et al.'s [127] (t, s, k, n)-ESIS scheme. However, both the schemes [21], [127] have limitations. The size of shadows is unequal, and the shadows' status based on size may leak secure information to the attackers. Another problem is when multiple subshadows are concatenated to get the last shadow, the reconstruction complexity increases. Further, Li et al. [128] have resolved the issue of different shadow sizes. In their scheme, each shadow has been generated by a single polynomial; thus, the size of essential shadows and non-essential shadows are the same. However, the concatenation of the subshadows problem is not solved. Chen [129] also provided another solution for the first problem of ESIS using a three-layered scheme, which can generate equal-sized essential and non-essential shadows. The scheme requires a very less amount of computation time too. To address both the problems, Li et al. [130] proposed another (t, k, n)-ESIS scheme. A (t, k, n)- ESIS scheme share a secret image using n shadows including t essential shadows and $(n - t)$ non-essential shadows. To reconstruct the secret image, at least k shadows are required, including all t essential shadows. In their scheme, all shadows have the size $\frac{1}{k}$ times of the secret image, and it also resolves the concatenation of the subshadows problem.

Recently, Sardar and Adhikari [131] proposed a (t, k, n)-ESIS scheme applicable for grayscale images over different field sizes. The scheme does not suffer from the problems of different shadow size, concatenation of subshadows, and the use of derivative polynomials. The scheme's main advantage is that it does not require any pre-processing step like random permutations or chaotic maps for security purposes. The proposed scheme over $GF(2^8)$ is completely lossless but little lossy over $GF(p^m)$ for $p^m > 2^8$. In essential SIS, recovering a secret image requires a threshold number of shares in addition to all necessary shares. Existing methods have some limitations, such as inconsistent share sizes, challenging computation, confusing random pattern sharing, explicit codebook requirements, pixel expansion, and image type limits. The applications of the SIS are constrained by these restrictions. The scheme proposed by [132] introduces a novel method of creating shares that are nearly the same size as the secret image. The ''essential SIS approach with same size of meaningful shares'' (ESISMS) scheme is a proposal that uses bitwise XORing to construct meaningful shares. In the following subsection we review the two-layered essential secret image sharing scheme proposed by Chen and Chen [133] which is based on the Thien-Lin [14] SIS scheme.

1) REVIEW OF CHEN AND CHEN'S ESIS SCHEME [133]

For simplicity, we present the share construction algorithm of Thien-Lin as an encryption function $E_{TL}(t, n, I_m)$ and secret image reconstruction algorithm as a decryption function $D_{TL}(t, n, \mathbf{S_m})$, where t is the threshold, n is the total number of shadows, I_m is the input image, and $\mathbf{S_m}$ is the set of input shadow images. The parameters of Chen and Chen's (t, s, k, n) ESIS scheme are as follows:

- The secret image I_s has to be encoded into n shadows.
- Out of n, s shared shadows are essential and $n-s$ shadows are non-essential.
- t-out-of-s essential shadows and totally k-out-of-n shared shadows are two threshold requirements to recover the secret image.

Construction Phase: The dealer D performs the following steps:

Step 1: Choose a permutation key K_p and permute the secret image I_s. Let the permuted secret image be I_s'.

Step 2: Call $E_{TL}(t+k, t+k, I_s')$ to generate $t+k$ *1st layered shadows*, $\{S_i'\}_{i=1}^{t+k}$.

Step 3: Concatenate $\{S_i'\}_{i=1}^{m}$ to obtain the *1st intermediate shadow*, I_1.

Step 4: Concatenate $\{S_i'\}_{i=m+1}^{t+k}$ to obtain the *2nd intermediate shadow*, I_2.

Step 5: Call $E_{TL}(t, s, I_1)$ to generate s *2st layered shadows*, $\{S_{1,i}'\}_{i=1}^{s}$.

Step 6: Call $E_{TL}(k, n, I_2)$ to generate n *2st layered shadows*, $\{S_{2,i}'\}_{i=1}^{n}$.

Step 7: Concatenate each pair of $\{S_{1,i}', S_{2,i}'\}_{i=1}^{s}$ to obtain the s essential Shadows $\{SI_e\}_{i=1}^{s}$.

Step 8: Assign each of $\{S_{2,i}'\}_{i=s+1}^{n}$ to $n-s$ non-essential shadows $\{SI_{ne}\}_{i=1}^{n-s}$.

Recovery Phase: Without loss of generality, we assume that t essential shadows $\{SI_e\}_{i=1}^{t}$ and $k-t$ non-essential shadows $\{SI_{ne}\}_{i=1}^{k-t}$ are available. The combine C reconstruct the secret image follows:

Step 1: For $i = 1$ to t Split each essential shadow SI_{e_i} to *2st layered shadows* $S_{1,i}'$ and $S_{2,i}'$.

Step 2: Call $D_{TL}(t, s, \{S_{1,i}'\}_{i=1}^{t})$ to recover the *1st intermediate shadow*, I_1 from $\{S_{1,i}'\}_{i=1}^{t}$.

Step 3: Call $D_{TL}(k, n, \{S_{2,i}'\}_{i=1}^{t} \cup SI_{ne_i}'\}_{i=1}^{k-t})$ to recover the *2nd intermediate shadow*, I_2 from $\{S_{2,i}'\}_{i=1}^{t}$ and $\{SI_{ne_i}\}_{i=1}^{k-t}$.

Step 4: Split the *intermediate shadow* I_1 to *1st layered shadows*, $\{S_i'\}_{i=1}^{m}$.

Step 5: Split the *intermediate shadow* I_2 to *1st layered shadows*, $\{S_i'\}_{i=m+1}^{t+k}$.

Step 6: Call $D_{TL}(t+k, t+k, \{S_i'\}_{i=1}^{t+k})$ to recover the permuted secret image I_s' from $\{S_i'\}_{i=1}^{t+k}$.

Step 7: Apply inverse permutation along with the permutation key K_p to recover the secret image I_s.

E. SCALABLE AND PROGRESSIVE SECRET IMAGE SHARING (SSIS AND PSIS)

In the traditional (t, n)-threshold SIS schemes, the secret image can be recovered in full if at least t of n share images are available. However, the secret image cannot be revealed in any way, if less than t share images are available. The limitation of this kind of scheme is that all participants hold the same amount of information, and based on threshold property, they either must recover the entire secret image or get nothing. Wang and Shyu [20] introduced a new kind of scheme named as *scalable SIS scheme* that shares a secret image such that the amount of information in the recovered secret image is proportional to the number of shadows used in the reconstruction process. They have defined three modes for sharing a secret image. They are as follows:

- **Multisecret mode**: The secret image is spatially partitioned into disjoint sub-images. Then, each sub-image is converted into a shadow image. Thus, the recovery of a particular portion of the secret image (sub-image) requires the involvement of the participant who holds the corresponding shadow image.
- **Priority mode**: The secret image is encoded into shadow images according to the bit-planes. The mode enables the dealer to specify the clarity of the reconstructed image to different groups of participants.
- **Progressive mode**: It is a combination of the multisecret and priority modes; The progressive mode provides multiple-resolution of a secret image. The quality of the recovered image is proportional to the number of shadows involved in the reconstruction. It is also referred to as progressive sharing.

The SSIS scheme proposed by Wang and Shyu [20] is a simple $(2, n)$ sharing method, and the size of each share image is half of the secret image. Yang and Huang [134] presented a (t, n) SSIS scheme, where $2 \le t \le n$. Another (t, n) SSIS scheme [135] is proposed by Lin and Wang, where the size of each generated share image is only $(2n-t)/n^2$ times the original image. As a result, it is better than Wang and Shyu's [20] scheme considering the size of the generated share images (or shadows). Several other (t, n) SSIS schemes in [136], [137], and [138] have smooth scalability. Liu et al. [139] proposed a new SIS scheme based on the concepts of bit-plane decomposition and Shamir's (t, n)-TSS scheme, which attains grouped and scalable management of a secret image. In the following subsection, we present a review of (t, n) scalable secret image sharing scheme by Lin and Wang [135].

F. REVIEW OF LIN AND WANG'S SSIS SCHEME [135]

Let the secret image be I_s.

Construction Phase: The dealer D performs the following:

Step 1: Split the secret image I_s into n disjoint image partitions $\{P_i\}_{i=1}^{n}$ such that the following properties hold.

1) $\bigcup\limits_i P_i = I_s$, for $1 \le i \le n$,
2) $P_i \cap P_j = \emptyset$, for $1 \le i \ne j \le n$,
3) $|P_i| = \frac{1}{n}|I_s|$, for $1 \le i \le n$ where $|\cdot|$ denotes the size of the image.

Step 2: For $j = 1$ to n, apply Thien-Lin $(n, 2n-t)$ on every partition image P_j to obtain $2n{-}t partitionshadows$ $\{s_{j,1}, s_{j,2}, \cdots, s_{j,2n-t}\}$.

Step 3: For $i = 1$ to n, obtain the *image shadow* S_i as follows:

$$S_i = \bigcup_j s_{j,k}, \text{ for } j = 1 \text{ to } n, \text{ where}$$

$$k = \begin{cases} j, j+1, \cdots, j+n-t, & \text{if } j = i, \\ i, & \text{if } j > i, \\ i+n-t, & \text{if } j < i. \end{cases}$$

Therefore, any image shadow S_i contains $n{-}t+1$ partition shadows of P_i and $n-1$ partition shadows from $n-1$

other partitions (one partition shadow from each of the other partitions). Since to recover any partition P_i at least n partition shadows (out of $2n-t$) are required, none of the image shadows reveal any information (any partition) about the secret image.

Recovery Phase: Each image shadow S_i contains $n-t+1$ partition shadows of partition P_i and one partition shadow for each partition P_j ($i \neq j$). As a result, combining any less than t image shadows reveals at most $n-1$ partition shadows of any partition, which means no partition can be recovered. However, if any $t+k$ ($k = 0, 1, \cdots, n-t$) image shadows are available, they contain at least n partition shadows of each of $t+k$ image partitions. Therefore, combining $t+k$ ($k = 0, 1, \cdots, n-t$) image shadows recovers the $t+k$ partition of the secret image I_s.

In a (t, n) *progressive SIS (PSIS) scheme*, a secret image is segmented into n share images, and t to n share images can progressively recover the secret image. The reconstructed image quality gradually increases with an increase in the number of shares submitted in the recovery process. There are two primary classifications of PSIS schemes: polynomial-based PSIS schemes and VC-based PSIS schemes. High-quality images are reconstructed in polynomial-based schemes; however, complex cryptographic computations are required for them. In VC-based PSIS schemes, the size of share images expands substantially from the secret image. The image quality is usually distorted when the image is reconstructed. However, the primary advantage of this kind of schemes is that no cryptographic computation is required to reconstruct the secret image(s). A polynomial-based PSIS scheme is discussed in [140] and various visual cryptography based PSIS schemes are discussed in [141], [142], [143], [144], [145], [146], and [147]. Liu et al. [148] proposed a (t, n) PSIS scheme based on Boolean operations. They have used the covering function from Hamming code to embed bits in pixels. This scheme generates smaller share images and higher-quality reconstructed images than previous visual cryptography-based PSIS schemes. Also, computational complexity is lower in this scheme in comparison with the previous polynomial based PSIS schemes. Chao and Fan [149] presented a priority-based visual secret sharing scheme (using random grid approach), which is free from pixel expansion and does not require any codebook. Additionally, it is capable of assigning each share a varying priority weight to create distinct priority levels. However, it has a problem of inconsistent contrast with different priority weights, which has an impact on the secret image's smooth progressive reconstruction [150]. To address this problem, Sridhar and Sudha [150] proposed two priority-based PSIS schemes: one with a codebook based approach and another with random-grid based approach. Yang et al. [26] proposed the first (t, n)-SIS scheme with a privileged set. They considered a privileged set of participants t_p in the scheme. The secret image can not only be revealed by any t out of n participants but also by t_p privileged participants, where $(t_p < t)$.

G. SIS SCHEMES WITH MEANINGFUL SHARES

Most of the SIS schemes generate all the shares in random patterns without visual information. These random-like share images may raise suspicions of possible data encryption among the attackers and attract them to perform cryptanalysis. Also, these meaningless shares are difficult to manage. To address the problem of random-like shares, a number of VSS schemes are presented in [151], [152], and [153] to generate meaningful shares. All of these schemes, however, struggle with image quality and dimension degradation issues. Ou et al. [117] presented a verifiable SIS scheme to generate meaningful shares based on block truncation coding (BTC) and error diffusion. The scheme has several merits: 1) no pixel expansion; 2) no requirement of codebooks; 3) BTC-compressed shares with smaller sizes; 4) meaningful shares that look almost the same as their original versions; 5) lossless recovery of the secret image; 5) XOR-based reconstruction with inexpensive computations; and 6) having the property of verification. Ou et al. [93] proposed an XOR-based (n, n) VSS scheme, which also does not require any extra processing to produce meaningful shares. Yan et al. [154] presented another SIS scheme based on the characteristic analysis of the secret image to produce meaningful shares without pixel expansion. Yan et al. [154] converted some of the classical SIS schemes with random-like (meaningless) shares to SIS schemes with meaningful shares. Yan et al. [155] presented a polynomial-based SIS scheme and a random grid-based VSS scheme with a general access structure to produce meaningful shares. Shivani [156] presented a MSIS scheme to share two secret images, producing meaningful shares without pixel expansion problem. Prior significant SIS schemes utilized steganography to conceal shares within cover images, which were always binary images. These schemes typically involve pixel expansion and shadows with poor visual quality. To enhance the quality of shadows, Cheng et al. [25] introduced a scheme for meaningful SIS with saliency detection. Saliency detection is utilized to identify the salient areas of cover images. The scheme enhanced the quality of salient regions that are receptive to the human visual system. The scheme acquires meaningful shadows with greater visual quality and significance. In the following section, we review the polynomial-based (t, n) threshold SIS Scheme with Meaningful Shares proposed by Yan et al. [154].

1) REVIEW OF YAN et al.'S SIS SCHEME [154]

The SIS construction method with meaningful shares is presented below.

Let us consider the following assumptions:

- An original secret image I_s with size of $(M \times N)$.
- The n binary cover images are denoted as $B_1, B_2, \cdots B_n$.
- The n shadows are denoted as $SI_1, SI_2, \cdots SI_n$.
- The shadow quality adjustment factor ϵ_0 and ϵ_1 corresponding to pixel value 0 and 1, respectively.

Also, note the following considerations:

- $I_s(m,n) \in [0, P-1]$ and $SI(m,n) \in [0, P-1]$ (for $1 \leq m \leq M$ and $1 \leq n \leq N$); where $[0, P-1]$ indicates the pixel value range and $(P-1)$ denotes the maximum pixel value.
- $Q(x, T_x)$ is the *binarization quantization function*, where T_x is the threshold determined by P in the existing SIS, such as, $T_x = (P-1)/2$.
- For the polynomial based scheme, if the secret pixel value is greater than 251, set it as 250. So, $I(m,n) \in [0, 250]$ and $T_x = 125$.

Construction Phase:

Step 1: For each position $(m,n) \in \{(m,n)|1 \leq m \leq M, 1 \leq n \leq N\}$, repeat Step 2.

Step 2: Let $s = I_s(m,n)$. If $s > P-1$, let $s = P-1$. Construct a $k-1$ degree polynomial as follows:

$$g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{t-1}x^{t-1} \; mod \; P \qquad (8)$$

subject to $Q(SI_i(m,n), T_i) = B_i(m,n)$ at probability $\epsilon_{B_i(m,n)}$, for $i = 1, 2, \cdots n$; where $a_0 = s$, a_i is random in $[0, P-1]$ for $i = 1, 2, \cdots, t-1$, $SI_1(m,n) = g(1), \cdots, SI_i(m,n) = g(i), \cdots, SI_n(m,n) = g(n)$, $P = 251$, $T_x = 125$ and

$$Q(x, T_x) = \begin{cases} 1, & \text{if } T_x \leq x, \\ 0, & \text{otherwise.} \end{cases}$$

Output: As a_i is generated randomly in $[0, P-1]$ for $i = 1, 2, \cdots, k-1$, thus a_i can be searched satisfying $Q(SI_i(m,n), T_i) = B_i(m,n)$ at probability $\epsilon_{B_i(a,b)}$, for $i = 1, 2, \cdots n$. Shadow pixels are affected by cover image pixels, allowing for the creation of n meaningful shadows $SI_1, SI_2, \cdots SI_n$.

VI. VERIFIABLE SECRET IMAGE SHARING (VSIS)

If appropriate precautions are not taken, SIS schemes are susceptible to various forms of cheating. Horng et al. [28] initially experimentally demonstrated that cheating is feasible in VC by forming a collusion of dishonest participants to deceive the honest participants. They proposed two different approaches to preventing cheating. In their first approach, extra shares were used to verify the validity of every share. In the second approach, they have developed a method that makes it exceedingly challenging for cheaters to predict the structure of the transparency held by genuine participants. De Prisco and De Santis [157] presented a $(2, n)$ VC scheme and a (n, n)-VC scheme, which can resist any cheating without requiring additional information (like extra shares or images) as required in [28]. In 2011, Liu et al. [29] proposed a cheating immune VC scheme with general access structure. This scheme is a low-cost scheme that works for both cases, whether the fundamental operation is OR or XOR. Another authentication-based cheating prevention scheme proposed by Chen et al. [158] comprises a share construction phase and a share verification phase. In this scheme, share transparencies are generated using the Naor-Shamir method [61]. Additionally, some black patterns are added to the stacking result so that the presence or absence of fake share transparency may be determined based on the quantity of black patterns. Chen et al. [92] analyzed the common cheating activities in the field of VSS and presented a detailed study of some of the important cheating prevention visual secret sharing schemes (CPVSS). They divided cheating into meaningful, non-meaningful, and meaningful deterministic. They have also proposed a CPVSS scheme to resist meaningful deterministic cheating. Their scheme also ensures a better result in terms of pixel expansion than most of the previous VSS schemes. Lin et al. [30] proposed another CPVSS scheme where the authentication pattern disclosed by partially stacking any pair of verifiable shares prevents cheating.

Cheating issues are not sufficiently discussed in the case of polynomial-based SIS and XOR-based SIS schemes. Most of the polynomial-based SIS schemes are based on Thien-Lin's [14] SIS scheme. Those schemes are mainly focused on reducing the size of the share images. However, the property of verifiability is missing from most of them. A polynomial-based verifiable (t, n)-threshold SIS scheme is presented by Zhao et al. [109], where security and verifiability are achieved by applying the method of the intractability of the DLP [159]. The scheme ensures that: 1) any cheating, either by the dealer or by the participants, can be detected and the cheaters can be identified; and 2) the share images can be distributed over public channels. Accordingly, the scheme does not assume that secure channels exist between the dealer and the participants; 3) the share images are still smaller than the secret image; and 4) it is a multi-use scheme as the same secret shadows, kept private with the participants, can be used in multiple sharing processes. However, the verification scheme is not computationally efficient. Liu et al. [31] presented another polynomial-based (t, n) SIS scheme, which can detect cheating by up to $(t-1)$ participants. The verification technique used in their scheme is based on polynomial interpolation only, and the size of each share image is $\frac{1}{(t-1)}$ times the size of the secret image. Furthermore, another cheating detection scheme that involves interpolation of linear polynomials is proposed by Ma et al. [110]. Nevertheless, this scheme further reduces the share size to $\frac{2}{(2t-1)}$ times of the secret image size and detects cheating by up to $t-1$ participants.

A very few XOR-based SIS schemes were proposed along with the verification property. Chattopadhyay et al. [32] presented one of such schemes that has the limited capability of identifying cheaters (participants only). Many verifiable SIS schemes employ hybrid approaches. A verifiable $(2, 2)$ SIS scheme presented by Chang et al. [160], is based on the halftoning transform, error diffusion, and image clustering techniques. However, the reconstruction and verification phases heavily depend on XOR operations. The scheme is applicable for binary, grayscale, and color images. Soreng and Kandar [33] proposed a VSIS scheme that is based on bitwise OR and XOR operations and hash functions. The proposed method is a (t, n) SS and can detect cheaters. Bitwise OR is used to perform the sharing, while XOR and

TABLE 6. Comparison between VSS, polynomial-based SIS and XOR-based SIS schemes.

	Visual Secret Sharing	Polynomial-based SIS	XOR-based SIS
Lossless recovery	Most of schemes are having lossy recovery of secret-image	Most of the schemes are lossy (however, the loss is very minute). For severe scheme lossless versions are also available.	Most of the schemes are lossless.
Pixel-expansion	Most of the schemes suffer from pixel-expansion problem.	No pixel-expansion problem.	No pixel-expansion problem.
Size of the share image	Larger or same as the secret image's size	For most of the schemes it is much lesser than the secret image	For most of the schemes it is same as the secret image.
Single or multi-secret sharing	Although a few basic schemes are for sharing single secret, most of the schemes are for sharing multiple secrets	Most of the schemes are single -secret sharing schemes	Most of the schemes are multi-secret sharing schemes
Threshold structure	The schemes are having either $(2, n)$-, (t, n)-, or (n, n)-threshold structures	Most of the schemes are having (t, n)-threshold structure	Most of the schemes are having $(2, n)$ and (n, n) structure
Computation required for *reconstruction of the secret(s)*	No or very little computation is required	Computation cost at reconstruction of the secret(s) is high. For basic schemes, it is usually $O(kt^2)$, where k is the number of blocks of t pixels from the secret image	Computation cost at reconstruction of the secret(s) is low. For basic schemes, it is usually $O(n)$, where n is number of total shares.
Verifiable	Many of schemes are verifiable	A very few schemes are verifiable.	A very few schemes are verifiable.

the hash operation are used to add verifiability. Another verifiable MSIS scheme based on secure hash functions was proposed by Chattopadhyay et al. [121], which applies hash functions in a cascaded manner to enable efficient verifications. In the following section, we briefly review the secret image sharing scheme presented by Zhao et al. [109], which is based on the Thien-Lin [14] scheme (reviewed in Section V-B1) and the intractability of the discrete logarithm.

A. REVIEW OF ZHAO et al.'S VSIS SCHEME [109]

Let the secret image be I_s. Similar to the Thien-Lin scheme, all the grayscale pixel values 251-255 of the original image are converted to 250 so that all the grayscale values are in the range [0-255]. Let the new image be I'.

Initialization Phase:

Step 1: The dealer D chooses two prime numbers, p and q, and computes $N_0 = pq$. The choice of p and q must ensure that factoring N_0 is hard.

Step 2: D also chooses an integer $g \in [N_0^{\frac{1}{2}}, N_0]$ such that g is coprime to p and q.

Step 3: D publishes $\{g, N_0\}$.

Step 4: Each participant $P_i \in \mathcal{P}$ randomly chooses an integer $w_i \in [2, N_0]$ as his secret shadow and computes $W_i = g^{w_i} \ mod \ N_0$. Each P_i transfers W_i to D.

Step 5: After receiving W_i from each $P_i \in \mathcal{P}$, D ensures that all W_i are unique; otherwise, D demands that all such P_is (all the P_i whose W_i are not unique) choose new w_is.

Construction Phase: D performs the following steps:

Step 1: Choose an integer $w_0 \in [2, N_0]$ such that w_0 is coprime to $(p-1)$ and $(q-1)$.

Step 2: Compute e such that $e \times w_0 = 1 \ mod \ \phi(N_0)$ where $\phi(N_0) = (p-1) \times (q-1)$.

Step 3: Compute $W_0 = g^{w_0} \ mod \ N_0$ and $X_i = W_i^{w_0} \ mod \ N_0, \ i = 1, 2, \cdots, n$. X_i is called the pseudo shadow for P_i. Publish $\{W_0, e\}$.

Step 4: Similar to the Thien-Lin scheme, generate a $(t-1)$ th degree polynomial $g_j(x)$ as follows:

$$g_j(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \ mod \ 251$$

where $\{a_i\}_{i=0}^{t-1}$ are the consecutive t pixels from the image section j.

Step 5: Evaluate $g_j(X_i)$ for $i = 1$ to n. Arrange the n pixels $\{g_j(i)\}_{i=1}^{n}$ from section j into n share images $\{SI_i\}_{i=1}^{n}$ sequentially, such that share image SI_i contains $g_j(X_i)$ for all sections j sequentially.

Step 6: Transmit each SI_i to P_i using some private channel.

Verification Phase:

Step 1: Any participant $P_i \in \mathcal{P}$ computes his pseudo shadow $X_i' = W_0^{w_i} \ mod \ N$, where w_i secret shadow of P_i.

Step 2: Anyone can check the legitimacy of X_i' that P_i has provided. If $X'^e = W_i \ mod \ N_0$ is true, then X_i' is valid ($X_i' = X_i$); otherwise, X_i' is fake, and P_i is a cheater.

Recovery Phase: Without loss of generality, if participants $\{P_i\}_{i=1}^{t}$ collaborate to recover the secret image, the polynomial $g_j(x)$ for each section j can be reconstructed as:

$$\begin{aligned} g_j(x) &= \sum_{i=1}^{t} g_j(X_i) \prod_{k=1}^{t} \frac{x - X_k'}{X_i' - X_k'} \ mod \ 251 \\ &= a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \ mod \ 251. \end{aligned}$$

Now, similar to the Thien-Lin scheme, arrange all the sections to recover the secret image I'. Since the secret shares are independently chosen by the participants, the dealer has no chance to become a cheater.

In Table 6, we have presented the merits and demerits of VSS schemes, polynomial-based SIS schemes, and XOR-based SIS schemes.

VII. SOME OTHER MISCELLANEOUS METHODS

There are numerous other methods proposed to implement secret sharing schemes. In this section, we discuss a few of them.

A. SECRET IMAGE SHARING BASED ON CELLULAR AUTOMATA

Cellular automata is a discrete dynamical model of computation used in a variety of secret sharing schemes. The idea of cellular automata is also utilized to implement different SIS schemes in [161] and [162]. Some SIS schemes [163], [164], [165] are presented using cellular automata and reversible steganography to achieve enhanced security.

B. DNA-BASED SECRET IMAGE SHARING

Anbarasi et al. [166] presented a DNA-based MSIS scheme with improved security. The authors used the concept of the YCH scheme [167] for multiple secret sharing and combined the algorithm with DNA encoding. Tuncer and Avci [168] proposed a DNA-XOR SS-based method for increasing the success rate of data-hiding techniques. Eswaran and Shankar [169] proposed a SIS scheme for enhancing the security of multiple digital images using DNA cryptography with XOR.

VIII. EVALUATION MATRICES OF SIS

In this section, important evaluation matrices for images are defined and discussed. Usually, image quality is assessed by the following metrics:

- **Correlation Coefficient**: Since a secret image stores a substantial amount of data, the correlations between the neighboring pixels in the image must be strong. However, correlations between the neighboring pixels are required to be significantly low in the share images [170]. Therefore, correlation analysis can be employed to determine whether or not the shared image is random (noise-like). The correlation coefficient must be very close to ±1 for a meaningful image, while it must be very close to 0 for a random image.

Let $\{x_i\}_{i=1}^n$ and $\{y_i\}_{i=1}^n$ be two sequences presenting n randomly selected adjacent pairs of pixels from a given grayscale image. The calculation of the correlation coefficient between these two sequences is as follows:

$$r_{x,y} = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\mu_x)(y_i-\mu_y)}{\sqrt{(\frac{1}{n}\sum_{i=1}^{n}(x_i-\mu_x)^2)(\frac{1}{n}\sum_{i=1}^{n}(y_i-\mu_y)^2)}}, \quad (9)$$

where μ_x and μ_y denote the means of x and y, respectively.

- **Entropy analysis**: It measures the unpredictability of information in a given image. A higher entropy value reflects less information and more randomness in the image [171]. For a given source m of n distinct symbols, the entropy $\mathcal{E}(m)$ is defined by the following formula:

$$\mathcal{E}(m) = -\sum_{i=0}^{n-1} P(m_1)\ log_2 P(m_i), \quad (10)$$

where $P(m_i)$ is the occurrence probability of the symbol m_i in m. In the case of a grayscale image $n = 256$. Thus, for an image to be considered really random, the entropy value needs to be very close to 8.

- **Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI)**: NPCR represents the percentage of different pixel numbers between any original image and the encrypted image, while UACI represents the average intensity of differences between the original image and the encrypted image. NPCR and UACI between two images, say, I_1 and I_2 of size $w \times h$ can be computed as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{w \times h} \times 100\%, \quad (11)$$

where

$$D(i,j) = \begin{cases} 1, & \text{if } I_1(i,j) \neq I_2(i,j), \\ 0, & \text{otherwise,} \end{cases}$$

and

$$UACI = \frac{1}{w \times h}\sum_{i,j}\frac{|I_1(i,j) - I_2(i,j)|}{255} \times 100\% \quad (12)$$

As per Wu et al. [172], the theoretical ideal NPCR and UACI values between two random images should be 99.6094% and 33.4635%, respectively.

- **Peak Signal-to-Noise Ratio (PSNR)**: The ratio of the original image to the encrypted image is the PSNR ratio. It compares the original and encrypted image quality. It calculates the ratio between maximum signal power and distorting noise power, which impacts its representation [173]. Most of the time, the logarithm of the decibel scale is used to figure out the PSNR. This is because the signals have a very wide dynamic range. This dynamic range changes between the highest and lowest possible numbers, whose quality can be changed. The quality of the compressed or encrypted image improves with increasing PSNR. PSNR is expressed as below:

$$PSNR = 10\log_{10}(peakval^2)/MSE,$$

where *peakval* (Peak Value) is the maximal in the image data and *MSE* is the *Mean Square Error*.

- **Structural Similarity Index Measure (SSIM)**: The SSIM value indicates the similarity and dissimilarity between two images [173]. It is related to Human visual system (HVS) quality perception. In this technique, image degradation changes structural information perception. SSIM models image distortion as luminance and contrast distortion instead of error summation. SSIM value 0 signifies the two images are completely different, and 1 implies they are identical. The SSIM index for images I_1 and I_2 of the same size is calculated as follows:

$$SSIM(I_1, I_2) = \frac{(2\mu_{I_1}\mu_{I_2} + C_1)(2\sigma_{I_1I_2} + c_2)}{(\mu_{I_1}^2 + \mu_{I_2}^2 + C_1)(\sigma_{I_1}^2 + \sigma_{I_2}^2 + c_2)} \quad (13)$$

where:

  - μ_{I_1} and μ_{I_2} are the mean intensities of I_1 and I_2,
  - $\sigma_{I_1}^2$ and $\sigma_{I_2}^2$ are the intensity-variance of I_1 and I_2,
  - $\sigma_{I_1I_2}$ is the intensities-covariance of I_1 and I_2,
  - C_1 and C_2 are two variables used for stabilizing the division with the weak denominator.

IX. APPLICATIONS

There are several real-life applications of SIS schemes. In this section, we briefly present some of them.

A. SECRET SHARING FOR QR-CODE APPLICATIONS

A QR (Quick Response) code is a symbol consisting of an array of approximately square components arranged uniquely in an overall square pattern. QR codes are frequently used to convey information that functions as a locator, an identifier, or a pointer that directs users to a certain internet site or service. In the scheme by Chow et al. [174], a QR code containing a confidential message is encoded as a collection of significant QR-code shares transmitted via printed media. Each share is a valid QR code when scanned one at a time. Each individual share produces a valid QR code that provides access to relevant information. As every share is a genuine QR code, when shares are disseminated through public channels, there is a lower probability that they will attract the attention of attackers. Individually, none of the shares can be used to decode the secret message. When all of the QR-code shares are available, it is possible to regenerate the original secret message. Cheng et al. [42] proposed a VSS scheme for QR-code. In their scheme, the secret message is recovered by performing the XOR operations between the qualified shares, which is attainable with the use of smartphones or other devices capable of scanning QR codes. Chuang et al. [175] proposed a SS scheme in order to improve the safety of users' data and maintain their privacy. The scheme is based on Shamir's SS scheme [7]. The secret message is encoded into some shares that are embedded into each QR-code tag. The scheme is secure because nobody can directly read the content of QR codes if the number of shares received is less than the predefined threshold. The approach is applicable to e-tickets, the inspection of luggage carried by airlines, and e-health systems for medical facilities. Liu et al. [176] used polynomial SS algorithms and proposed a two-level QR code that protects secret messages based on QR code machine recognition features. The scheme is flexible, as it can recover secret information even if a portion of the two-level QR code is broken for any reason. The storage capacity of the secret message is also very high in this scheme. The scheme has real-life applications in the logistics industry, hospitals, and many other places to protect users' sensitive information. Yu et al. [43] proposed a high-capacity QR code associated with three-layer information to secure private data using an XOR-based SS algorithm. This scheme can be utilized to protect the medical records of patients in any hospital. Huang et al. [177] proposed a practical threshold SS method with the ability to detect cheaters utilizing meaningful QR codes. The fault tolerance property of the scheme would enable it to generate meaningful QR code shares, which would then be used to conceal the shares it generates within cover QR codes. Meaningful QR code shares can be useful in avoiding the attention of attackers when transmitted through a public channel. The authenticity of the QR code share would be checked before the secret reconstruction in order to prevent cheating. Wan et al. [178] proposed a VSS scheme using QR codes (VSSQR) with a (t, n)-threshold structure. A secret image is encoded into n QR code shares and distributed. The secret image can be recovered by staking any t or more QR codes with a QR code reader. The scheme utilizes an error correction mechanism in the QR code structure. Since the scheme uses XOR-based decoding for the recovery of secrets, it incurs very low computation costs. Thus, any lightweight device can be utilized for secret reconstruction. The scheme also produces a high-quality secret image due to lossless recovery. Tan et al. [179] introduced an XOR-based (t, n)-threshold VSS scheme using QR codes. The scheme is robust, has error correction capability, and has a low computation requirement.

B. SECRET SHARING FOR MEDICAL IMAGE SECURITY

In a medical information system [180], an extensive collection of medical images like reports of MRI scans, CT scans, Ultrasound scans, X-rays, etc. are generated, which are frequently required to be stored and communicated on the public networks connecting hospitals, clinics, diagnosis centers, etc. As these images contain sensitive information about the patients, the protection of the medical images is the greatest concern in medical information systems. The disclosure or theft of patients' health information from medical images may have severe consequences for individual patients and healthcare professionals. It may even endanger the patient's life. Ulutas et al. [17] presented a scheme that securely transfers medical images over a public network among medical professionals based on Shamir's [7] SS. The scheme [181] introduced by Krishnan et al. is based on the concept of Ulutas et al. [17] which has additional features for detection of cheating and identification of the cheater. The proposed scheme protects medical images from unlawful ingress and detects cheating among the participating clinicians, if any. To protect the privacy of medical images, Tso and Lou [180] presented a VSS scheme using the multi-bit grid concept. The scheme is a lossless scheme; thus, it guarantees that no information is lost in the sharing process. Another VSS-based approach is proposed in [182] for the security and privacy of black and white medical images. In this technique, a $(2, 2)$ VSS scheme is used to produce two share images from a secret medical image such that the individual share image does not disclose any details regarding the secret medical image. Therefore, the share images can be safely transferred over an insecure network. The secret medical image can only be reconstructed whenever two shares are stacked together. This scheme may be applied to maintain the privacy of Electronic Medical Reports (EMR) and medical images, from which sensitive information can be revealed or tampered with by any unauthorized person.

Kanso and Ghebleh [183] presented a polynomial-based SIS scheme for medical images. The scheme is entirely lossless. The scheme applies a customized run-length encoding method for compressing the medical image and generates shares using the same concept as Thien and Lin's [14] scheme. In this scheme, the share size is reduced by compressing the secret image, which is suitable for storage and transmission. Maurya et al. [44] proposed an extended visual cryptography technique (EVCT) for medical image security. The scheme enables the secure transmission of medical images over a trusted or untrusted medium. In this scheme, the secret medical image is encrypted using the circular shift encryption (CSE) algorithm and embedded into three cover images to produce three meaningful shares. Then, the meaningful shares are transferred over a public network. The secret image can be reconstructed from those three meaningful shares, followed by its decryption at the receiver's end. Personal Health Records (PHR) and storage data centers process large amounts of health data due to the exponential rise of the Internet of Health Things (IoHT) in health systems. The security of this massive medical data is a serious issue. The scheme introduced by Sarosh et al. [44] generates key and image shares that are entirely noise-like and spread across numerous servers in an IoHT-based framework. By performing this, single-point attacks on the cryptosystem are avoided. The proposed method recovers medical data without introducing any loss, assisting in data analysis and diagnosis in IoHT.

In the COVID-19 pandemic situation, when social distancing has become mandatory, *telehealth* plays an essential role as it bridges physical distance between patients, clinicians, and other entities of the healthcare system. Sarkar and Sarkar [184] introduced a SS-based technique to improve the security of the existing *telehealth* system. They have presented a (t, n) patients' privileged-based SS scheme for secure communication of electronic medical records. It ensures that the t or more valid shares presented in the reconstruction process must include one share (privileged share) from a specified participant (a patient) in order to regenerate the original secret. The use of Tree Parity Machine (TPM)-based exchange of shares successfully prevents the man-in-the-middle (MITM) attack.

X. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

The open challenges and future research directions of SIS are diverse and require multidisciplinary research efforts involving different research areas of computer science.

- A few XOR-based (t, n)-threshold SIS schemes are presented; however, they have several limitations. Designing XOR-based SIS schemes with a real (t, n)-threshold structure is yet an open challenge.
- XOR-based SIS schemes are computationally efficient and perform completely lossless reconstruction; however, for most of these schemes, the share size (which is the same as the secret's size) is a limitation. A few XOR-based SIS schemes are available that can generate smaller shares, applicable only for single image sharing. Hence, there is scope to develop coherent XOR-based SIS schemes that can reduce the size of shares significantly.
- Most of the XOR-based SIS schemes use some pseudo-random generator (PRG) to generate random images to be used to produce the share images. Therefore, the security of share images is highly dependent on the security of the PRG function used in the scheme. Therefore, designing XOR-based SIS schemes without using PRG functions is an open challenge.
- Most of the polynomial-based SIS schemes cannot randomize the share images effectively. Therefore, they usually involve some prepossessing to randomize the pixels of secret images before the shares are constructed, which is definitely an overhead. Better approaches can be developed if the randomization can be achieved by the share construction method itself. Some studies have been performed in the area. However, it is still an open field of research.
- Most SIS techniques have high computational and storage costs, making them unsuitable for large-scale image sharing applications. Future research can focus on developing efficient SIS techniques that can scale to handle large images and high volumes of image data.
- Most SIS techniques rely on the assumption that the shares are kept secret and cannot be tampered with. However, recent studies have shown that some SIS techniques are vulnerable to attacks such as collusion attacks, watermarking attacks, etc. Future research can focus on developing more secure SIS techniques that can resist these attacks.
- SIS techniques can be exposed to a variety of factors, such as noise, compression, and cropping, which can affect the quality and authenticity of the shares. Future research can focus on developing SIS techniques that are robust to such distortions and can recover the original image accurately.
- There are currently no standardized formats for SIS shares, making it difficult to distribute shares (or shadows) and combine shares (or shadows) generated by different techniques. Future research can focus on developing interoperable SIS formats that can be used by different SIS techniques and applications.
- Most SIS techniques require all the shares to be gathered to regenerate the original image, making them unsuitable for privacy-preserving applications where only certain parts of the image need to be revealed. Future research can focus on developing SIS techniques that can selectively reveal parts of the image while keeping the remaining parts secret.
- SIS techniques can take a long time to generate shares and regenerate the actual image, making them unsuitable for real-time applications. Future research can focus on developing SIS techniques that can generate shares and reconstruct images in real-time, making them suitable for applications such as video streaming and real-time surveillance.
- Different applications may have different requirements for SIS, such as the number of shares, the threshold for reconstruction, and the level of security. Future research can concentrate on developing SIS techniques that can be tailored to specific applications and their requirements.

XI. CONCLUSION

This survey paper presents a comprehensive overview of the current state of research in secret image sharing (SIS). We have discussed the fundamental concepts of SIS, presented an in-depth analysis of various SIS techniques, and emphasized their strengths and weaknesses. We have briefly studied the new technologies evolving in this field. We have also summarized several applications based on SIS schemes. In addition, we have discussed the challenges and future research directions of SIS, including scalability, security, interoperability, privacy-preserving SIS, real-time SIS, and application-specific SIS. Our analysis has revealed that SIS is a promising technique that offers a range of benefits, including confidentiality, integrity, and authenticity. However, there are still several open challenges that need to be addressed to make SIS schemes more practical and efficient. Researchers can focus on developing more secure, scalable, and efficient SIS techniques that can meet the requirements of different applications. The future research section, which we have discussed in this work, can concentrate on developing innovative SIS schemes in the future. Overall, this survey paper can serve as an informative resource for researchers who are interested in the field of SIS. It provides a holistic view of the field, highlights the challenges and open research directions, and can guide future research efforts.

REFERENCES

[1] S. Dey, "SD-EI: A cryptographic technique to encrypt images," in *Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic (CyberSec)*, Jun. 2012, pp. 28–32.

[2] Q.-A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, and N. N. Quaynor, "A cryptographic technique for security of medical images in health information systems," *Proc. Comput. Sci.*, vol. 58, pp. 538–543, Jan. 2015.

[3] M. Mundher, D. Muhamad, A. Rehman, T. Saba, and F. Kausar, "Digital watermarking for images security using discrete slantlet transform," *Appl. Math. Inf. Sci.*, vol. 8, no. 6, pp. 2823–2830, Nov. 2014.

[4] A. Mohanarathinam, "Digital watermarking techniques for image security: A review," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 8, pp. 3221–3229, 2020.

[5] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[6] M. Idakwo, M. Muazu, E. Adedokun, and B. Sadiq, "An extensive survey of digital image steganography: State of the art," *ATBU J. Sci., Technol. Educ.*, vol. 8, no. 2, pp. 40–54, 2020.

[7] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[8] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl. (MARK)*, 1979, pp. 313–318.

[9] M. Mignotte, "How to share a secret," in *Proc. Workshop Cryptogr.* Cham, Switzerland: Springer, 1982, pp. 371–375.

[10] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 208–210, Mar. 1983.

[11] C. S. Chum, B. Fine, G. Rosenberger, and X. Zhang, "A proposed alternative to the Shamir secret sharing scheme," *Contemp. Math.*, vol. 582, pp. 47–50, Jan. 2012.

[12] K. E. Atkinson, *An Introduction to Numerical Analysis*. Hoboken, NJ, USA: Wiley, 2008.

[13] B. Fine, A. I. S. Moldenhauer, and G. Rosenberger, "A secret sharing scheme based on the closest vector theorem and a modification to a private key cryptosystem," *Groups-Complex.-Cryptol.*, vol. 5, no. 2, pp. 223–238, Jan. 2013.

[14] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, Oct. 2002.

[15] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," *Comput. Standards Interface*, vol. 29, no. 1, pp. 138–141, Jan. 2007.

[16] L. Harn and C. Lin, "Detection and identification of cheaters in (t, n) secret sharing scheme," *Des., Codes Cryptogr.*, vol. 52, no. 1, pp. 15–24, Jul. 2009.

[17] M. Ulutas, G. Ulutas, and V. V. Nabiyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme," *J. Syst. Softw.*, vol. 84, no. 3, pp. 341–353, Mar. 2011.

[18] A. Basit, N. C. Kumar, V. Ch. Venkaiah, S. A. Moiz, A. N. Tentu, and W. Naik, "Multi-stage multi-secret sharing scheme for hierarchical access structure," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, May 2017, pp. 557–563.

[19] C.-C. Lin and W.-H. Tsai, "Secret image sharing with steganography and authentication," *J. Syst. Softw.*, vol. 73, no. 3, pp. 405–414, Nov. 2004.

[20] R.-Z. Wang and S.-J. Shyu, "Scalable secret image sharing," *Signal Process., Image Commun.*, vol. 22, no. 4, pp. 363–373, Apr. 2007.

[21] C.-N. Yang, P. Li, C.-C. Wu, and S.-R. Cai, "Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach," *Signal Process., Image Commun.*, vol. 31, pp. 1–9, Feb. 2015.

[22] C.-C. Chen and W.-J. Wu, "A secure Boolean-based multi-secret image sharing scheme," *J. Syst. Softw.*, vol. 92, pp. 107–114, Jun. 2014.

[23] H. Prasetyo and J.-M. Guo, "A note on multiple secret sharing using Chinese remainder theorem and exclusive-OR," *IEEE Access*, vol. 7, pp. 37473–37497, 2019.

[24] M. Deshmukh, N. Nain, and M. Ahmed, "A novel approach for sharing multiple color images by employing Chinese remainder theorem," *J. Vis. Commun. Image Represent.*, vol. 49, pp. 291–302, Nov. 2017.

[25] J. Cheng, X. Yan, L. Liu, Y. Jiang, and X. Wang, "Meaningful secret image sharing with saliency detection," *Entropy*, vol. 24, no. 3, p. 340, Feb. 2022.

[26] C.-N. Yang, P. Li, and H.-C. Kuo, "(k, n) secret image sharing scheme with privileged set," *J. Inf. Secur. Appl.*, vol. 73, Mar. 2023, Art. no. 103413.

[27] X. Wu and P. Yao, "Boolean-based two-in-one secret image sharing by adaptive pixel grouping," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 19, no. 1, pp. 1–23, 2023.

[28] G. Horng, T. Chen, and D.-S. Tsai, "Cheating in visual cryptography," *Des., Codes Cryptogr.*, vol. 38, no. 2, pp. 219–236, Feb. 2006.

[29] F. Liu, C. Wu, and X. Lin, "Cheating immune visual cryptography scheme," *IET Inf. Secur.*, vol. 5, no. 1, pp. 51–59, 2011.

[30] P.-Y. Lin, R.-Z. Wang, Y.-J. Chang, and W.-P. Fang, "Prevention of cheating in visual cryptography by using coherent patterns," *Inf. Sci.*, vol. 301, pp. 61–74, Apr. 2015.

[31] Y.-X. Liu, Q.-D. Sun, and C.-N. Yang, "(k,n) secret image sharing scheme capable of cheating detection," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 72, Dec. 2018.

[32] A. K. Chattopadhyay, D. Ghosh, P. Maitra, A. Nag, and H. N. Saha, "A verifiable (n, n) secret image sharing scheme using XOR operations," in *Proc. 9th IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Nov. 2018, pp. 1025–1031.

[33] A. V. Soreng and S. Kandar, "A verifiable threshold secret image sharing (SIS) scheme with combiner verification and cheater identification," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 8, pp. 1–25, 2022.

[34] O. O. Bamasag and K. Youcef-Toumi, "Towards continuous authentication in Internet of Things based on secret sharing scheme," in *Proc. Workshop Embedded Syst. Secur.*, 2015, pp. 1–8.

[35] W. Zheng, K. Wang, and F.-Y. Wang, "GAN-based key secret-sharing scheme in blockchain," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 393–404, Jan. 2021.

[36] S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "Accountable privacy preserving attribute based framework for authenticated encrypted access in clouds," *J. Parallel Distrib. Comput.*, vol. 135, pp. 1–20, Jan. 2020.

[37] X. Tan, J. Zheng, C. Zou, and Y. Niu, "Pseudonym-based privacy-preserving scheme for data collection in smart grid," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 22, no. 2, pp. 120–127, 2016.

[38] Y. Chen, F. Luo, T. Li, T. Xiang, Z. Liu, and J. Li, "A training-integrity privacy-preserving federated learning scheme with trusted execution environment," *Inf. Sci.*, vol. 522, pp. 69–79, Jun. 2020.

[39] F. Sattler, S. Wiedemann, K.-R. Müller, and W. Samek, "Robust and communication-efficient federated learning from non-i.i.d. Data," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 9, pp. 3400–3413, Sep. 2020.

[40] S. Iftene, "General secret sharing based on the Chinese remainder theorem with applications in e-voting," *Electron. Notes Theor. Comput. Sci.*, vol. 186, pp. 67–84, Jul. 2007.

[41] P.-A. Fouque, G. Poupard, and J. Stern, "Sharing decryption in the context of voting or lotteries," in *Proc. Int. Conf. Financial Cryptogr.* Cham, Switzerland: Springer, 2000, pp. 90–104.

[42] Y. Cheng, Z. Fu, and B. Yu, "Improved visual secret sharing scheme for QR code applications," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2393–2403, Sep. 2018.

[43] B. Yu, Z. Fu, and S. Liu, "A novel three-layer QR code based on secret sharing scheme and liner code," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, Nov. 2019.

[44] R. Maurya, A. K. Kannojiya, and B. Rajitha, "An extended visual cryptography technique for medical image security," in *Proc. 2nd Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA)*, Mar. 2020, pp. 415–421.

[45] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 1994, pp. 1–12.

[46] C.-C. Wu and L. Chen, "A study on visual cryptography," Ph.D. thesis, Inst. Comput. Inf. Sci., Nat. Chiao Tung Univ., Hsinchu, Taiwan, 1998.

[47] T. Katoh and H. Imai, "An extended construction method for visual secret sharing schemes," *Electron. Commun. Jpn., III, Fundam. Electron. Sci.*, vol. 81, no. 7, pp. 55–63, Jul. 1998.

[48] H.-C. Wu and C.-C. Chang, "Sharing visual multi-secrets using circle shares," *Comput. Standards Interface*, vol. 28, no. 1, pp. 123–135, Jul. 2005.

[49] H.-C. Hsu, T.-S. Chen, and Y.-H. Lin, "The ringed shadow image technology of visual cryptography by applying diverse rotating angles to bide the secret sharing," in *Proc. IEEE Int. Conf. Netw., Sens. Control*, Mar. 2004, pp. 996–1001.

[50] S. J. Shyu, S.-Y. Huang, Y.-K. Lee, R.-Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognit.*, vol. 40, no. 12, pp. 3633–3651, Dec. 2007.

[51] Z. Fu and B. Yu, "Research on rotation visual cryptography scheme," in *Proc. Int. Symp. Inf. Eng. Electron. Commerce*, May 2009, pp. 533–536.

[52] T.-H. Chen, K.-H. Tsao, and Y.-S. Lee, "Yet another multiple-image encryption by rotating random grids," *Signal Process.*, vol. 92, no. 9, pp. 2229–2237, Sep. 2012.

[53] S. J. Shyu, "Image encryption by random grids," *Pattern Recognit.*, vol. 40, no. 3, pp. 1014–1031, Mar. 2007.

[54] C.-L. Liu, W.-J. Tsai, T.-Y. Chang, C.-C. Peng, and P.-S. Wong, "Meaningful share generation for (2, 2)-multiple visual secret sharing scheme without pixel expansion," *Comput. J.*, vol. 58, no. 7, pp. 1598–1606, Jul. 2015.

[55] T.-S. Chen, "New visual cryptography system based on circular shadow image and fixed angle segmentation," *J. Electron. Imag.*, vol. 14, no. 3, Jul. 2005, Art. no. 033018.

[56] C.-N. Yang and T.-S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 21, no. 5, pp. 879–898, Aug. 2007.

[57] S.-K. Chen, "A visual cryptography based system for sharing multiple secret images," in *Proc. ISCGAV*, vol. 7, 2007, pp. 117–122.

[58] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-F. Chang, and Y.-P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognit.*, vol. 41, no. 12, pp. 3572–3581, Dec. 2008.

[59] S. J. Shyu and K. Chen, "Visual multiple secret sharing based upon turning and flipping," *Inf. Sci.*, vol. 181, no. 15, pp. 3246–3266, Aug. 2011.

[60] A. Mishra and A. Gupta, "Multi secret sharing scheme using iterative method," *J. Inf. Optim. Sci.*, vol. 39, no. 3, pp. 631–641, Apr. 2018.

[61] M. Naor and A. Shamir, "Visual cryptography II: Improving the contrast via the cover base," in *Proc. Int. Workshop Secur. Protocols*. Cham, Switzerland: Springer, 1996, pp. 197–202.

[62] V. Rijmen, "Efficient color visual encryption or 'shared colors of Benetton,"' in *Proc. EUROCRYPT*, 1996, pp. 1–12.

[63] C.-N. Yang, "A note on efficient color visual encryption," *J. Inf. Sci. Eng.*, vol. 18, no. 3, pp. 367–372, 2002.

[64] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognit.*, vol. 36, no. 7, pp. 1619–1629, Jul. 2003.

[65] E. R. Verheul and H. C. A. van Tilborg, "Constructions and properties of *k* out of *n* visual secret sharing schemes," *Des., Codes Cryptogr.*, vol. 11, no. 2, pp. 179–196, 1997.

[66] H. Koga and H. Yamamoto, "Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 81, no. 6, pp. 1262–1269, 1998.

[67] C.-N. Yang and C.-S. Laih, "New colored visual secret sharing schemes," *Des., Codes Cryptogr.*, vol. 20, no. 3, pp. 325–336, 2000.

[68] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," *Des., Codes Cryptogr.*, vol. 24, no. 3, pp. 255–278, 2001.

[69] T.-H. Chen and K.-H. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1693–1703, Nov. 2011.

[70] T.-H. Chen and K.-H. Tsao, "Threshold visual secret sharing by random grids," *J. Syst. Softw.*, vol. 84, no. 7, pp. 1197–1208, Jul. 2011.

[71] X. Yan, S. Wang, A. A. A. El-Latif, and X. Niu, "Random grids-based visual secret sharing with improved visual quality via error diffusion," *Multimedia Tools Appl.*, vol. 74, no. 21, pp. 9279–9296, Nov. 2015.

[72] X. Yan, S. Wang, A. A. A. El-Latif, and X. Niu, "Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery," *Multimedia Tools Appl.*, vol. 74, no. 9, pp. 3231–3252, May 2015.

[73] X. Yan, X. Liu, and C.-N. Yang, "An enhanced threshold visual secret sharing based on random grids," *J. Real-Time Image Process.*, vol. 14, no. 1, pp. 61–73, Jan. 2018.

[74] A. Adhikari, "Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images," *Des., Codes Cryptogr.*, vol. 73, no. 3, pp. 865–895, Dec. 2014.

[75] S. Cimato, R. D. Prisco, and A. D. Santis, "Optimal colored threshold visual cryptography schemes," *Des., Codes Cryptogr.*, vol. 35, no. 3, pp. 311–335, Jun. 2005.

[76] T.-H. Chen and C.-S. Wu, "Efficient multi-secret image sharing based on Boolean operations," *Signal Process.*, vol. 91, no. 1, pp. 90–97, Jan. 2011.

[77] S. Cimato, R. De Prisco, and A. De Santis, "Colored visual cryptography without color darkening," *Theor. Comput. Sci.*, vol. 374, nos. 1–3, pp. 261–276, Apr. 2007.

[78] S. J. Shyu and M. C. Chen, "Optimum pixel expansions for threshold visual secret sharing schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 960–969, Sep. 2011.

[79] S. Dutta and A. Adhikari, "Contrast optimal XOR based visual cryptographic schemes," in *Proc. Int. Conf. Inf. Theoretic Secur.* Cham, Switzerland: Springer, 2017, pp. 58–72.

[80] S. Dutta, A. Adhikari, and S. Ruj, "Maximal contrast color visual secret sharing schemes," *Des., Codes Cryptogr.*, vol. 87, no. 7, pp. 1699–1711, Jul. 2019.

[81] I. Muecke, "Greyscale and colour visual cryptography," M.S. thesis, Dept. Comput. Sci., Dalhouse Uinversity-Daltech, Halifax, NS, Canada, 2000.

[82] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," *Inf. Process. Lett.*, vol. 75, no. 6, pp. 255–259, Nov. 2000.

[83] A. Adhikari and S. Sikdar, "A new (2,*n*)-visual threshold scheme for color images," in *Proc. Int. Conf. Cryptol.* Cham, Switzerland: Springer, 2003, pp. 148–161.

[84] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fundamentals Electron. Commun. Comput. Sci.*, vol. 82, no. 10, pp. 2172–2177, 1999.

[85] Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," *Inf. Sci.*, vol. 177, no. 21, pp. 4696–4710, Nov. 2007.

[86] C.-N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, Mar. 2004.

[87] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes," *Comput. J.*, vol. 49, no. 1, pp. 97–107, Jan. 2006.

[88] D. Wang, L. Zhang, N. Ma, and X. Li, "Two secret sharing schemes based on Boolean operations," *Pattern Recognit.*, vol. 40, no. 10, pp. 2776–2785, Oct. 2007.

[89] C.-C. Chang, C.-C. Lin, T. H. N. Le, and H. B. Le, "A new probabilistic visual secret sharing scheme for color images," in *Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Aug. 2008, pp. 1305–1308.

[90] C.-C. Chang and M.-N. Wu, "An algorithm for color image compression base on common bit map block truncation coding," in *Proc. JCIS*, 2002, pp. 964–967.

[91] C.-C. Chang, C.-C. Lin, T. H. N. Le, and H. B. Le, "A probabilistic visual secret sharing scheme for grayscale images with voting strategy," in *Proc. Int. Symp. Electron. Commerce Secur.*, 2008, pp. 184–188.

[92] Y.-C. Chen, D.-S. Tsai, and G. Horng, "Visual secret sharing with cheating prevention revisited," *Digit. Signal Process.*, vol. 23, no. 5, pp. 1496–1504, Sep. 2013.

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

[94] R. De Prisco and A. De Santis, "Color visual cryptography schemes for black and white secret images," *Theor. Comput. Sci.*, vol. 510, pp. 62–86, Oct. 2013.

[95] X. Wu and C.-N. Yang, "Probabilistic color visual cryptography schemes for black and white secret images," *J. Vis. Commun. Image Represent.*, vol. 70, Jul. 2020, Art. no. 102793.

[96] C.-C. Lin and W.-H. Tsai, "Secret image sharing with capability of share data reduction," *Opt. Eng.*, vol. 42, no. 8, pp. 2340–2345, 2003.

[97] C. Chang, C. Lin, C. Lin, and Y. Chen, "A novel secret image sharing scheme in color images using small shadow images," *Inf. Sci.*, vol. 178, no. 11, pp. 2433–2447, Jun. 2008.

[98] R.-Z. Wang and C.-H. Su, "Secret image sharing with smaller shadow images," *Pattern Recognit. Lett.*, vol. 27, no. 6, pp. 551–555, 2006.

[99] K.-S. Wu, "A secret image sharing scheme for light images," *EURASIP J. Adv. Signal Process.*, vol. 2013, no. 1, pp. 1–5, Dec. 2013.

[100] A. Kanso and M. Ghebleh, "An efficient (t,n)—Threshold secret image sharing scheme," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16369–16388, 2017.

[101] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 235–246, Feb. 2016.

[102] Z. Zhou, C.-N. Yang, Y. Cao, and X. Sun, "Secret image sharing based on encrypted pixels," *IEEE Access*, vol. 6, pp. 15021–15025, 2018.

[103] M. Ghebleh and A. Kanso, "A novel secret image sharing scheme using large primes," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 11903–11923, May 2018.

[104] N. F. Azzahra and K. A. Sugeng, "Verifiable image secret sharing using matrix projection," *J. Phys., Conf. Ser.*, vol. 1108, Nov. 2018, Art. no. 012082.

[105] M. K. Sardar and A. Adhikari, "A new lossless secret color image sharing scheme with small shadow size," *J. Vis. Commun. Image Represent.*, vol. 68, Apr. 2020, Art. no. 102768.

[106] P. K. Meher and J. C. Patra, "A new approach to secure distributed storage, sharing and dissemination of digital image," in *Proc. IEEE Int. Symp. Circuits Syst.*, Feb. 2006, pp. 1–4.

[107] S. J. Shyu and Y.-R. Chen, "Threshold secret image sharing by Chinese remainder theorem," in *Proc. IEEE Asia–Pacific Services Comput. Conf.*, Dec. 2008, pp. 1332–1337.

[108] C.-C. Chang, N.-T. Huynh, and H.-D. Le, "Lossless and unlimited multi-image sharing based on Chinese remainder theorem and Lagrange interpolation," *Signal Process.*, vol. 99, pp. 159–170, Jun. 2014.

[109] R. Zhao, J.-J. Zhao, F. Dai, and F.-Q. Zhao, "A new image secret sharing scheme to identify cheaters," *Comput. Standards Interface*, vol. 31, no. 1, pp. 252–257, Jan. 2009.

[110] J. Ma, L. Yin, and P. Li, "Cheating detection in (k,n) secret image sharing scheme," in *Proc. Int. Workshop Digit. Watermarking*. Cham, Switzerland: Springer, 2019, pp. 421–428.

[111] C.-N. Yang, C.-H. Chen, and S.-R. Cai, "Enhanced Boolean-based multi secret image sharing scheme," *J. Syst. Softw.*, vol. 116, pp. 22–34, Jun. 2016.

[112] C.-C. Chen, W.-J. Wu, and J.-L. Chen, "Highly efficient and secure multi-secret image sharing scheme," *Multimedia Tools Appl.*, vol. 75, no. 12, pp. 7113–7128, Jun. 2016.

[113] C. Guo, H. Zhang, Q. Song, and M. Li, "A multi-threshold secret image sharing scheme based on the generalized Chinese reminder theorem," *Multimedia Tools Appl.*, vol. 75, no. 18, pp. 11577–11594, Sep. 2016.

[114] K. M. Faraoun, "Design of a new efficient and secure multi-secret images sharing scheme," *Multimedia Tools Appl.*, vol. 76, no. 5, pp. 6247–6261, Mar. 2017.

[115] C.-C. Chen and J.-L. Chen, "A new Boolean-based multiple secret image sharing scheme to share different sized secret images," *J. Inf. Secur. Appl.*, vol. 33, pp. 45–54, Apr. 2017.

[116] S. Kabirirad and Z. Eslami, "Improvement of (n, n)-multi-secret image sharing schemes based on Boolean operations," *J. Inf. Secur. Appl.*, vol. 47, pp. 16–27, Aug. 2019.

[117] D. Ou, L. Ye, and W. Sun, "User-friendly secret image sharing scheme with verification ability based on block truncation coding and error diffusion," *J. Vis. Commun. Image Represent.*, vol. 29, pp. 46–60, May 2015.

[118] S. Kabirirad and Z. Eslami, "A (t, n)-multi secret image sharing scheme based on Boolean operations," *J. Vis. Commun. Image Represent.*, vol. 57, pp. 39–47, Jan. 2018.

[119] H. Prasetyo and C.-H. Hsia, "Lossless progressive secret sharing for grayscale and color images," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24837–24862, Sep. 2019.

[120] A. Nag, J. P. Singh, and A. K. Singh, "An efficient Boolean based multi-secret image sharing scheme," *Multimedia Tools Appl.*, vol. 76, pp. 1–25, Jan. 2019.

[121] A. K. Chattopadhyay, A. Nag, J. P. Singh, and A. K. Singh, "A verifiable multi-secret image sharing scheme using XOR operation and hash function," *Multimedia Tools Appl.*, vol. 80, pp. 1–30, Jan. 2020.

[122] A. K. Chattopadhyay, A. Nag, and J. P. Singh, "An efficient verifiable (t,n)-threshold secret image sharing scheme with ultralight shares," *Multimedia Tools Appl.*, vol. 2021, pp. 1–31, Feb. 2021.

[123] M. Deshmukh, N. Nain, and M. Ahmed, "Efficient and secure multi secret sharing schemes based on Boolean XOR and arithmetic modulo," *Multimedia Tools Appl.*, vol. 77, no. 1, pp. 89–107, Jan. 2018.

[124] C.-C. Chen, "Weighted modulated secret image sharing method," *J. Electron. Imag.*, vol. 18, no. 4, Oct. 2009, Art. no. 043011.

[125] S. J. Shyu, C.-C. Chuang, Y.-R. Chen, and A.-F. Lai, "Weighted threshold secret image sharing," in *Proc. Pacific-Rim Symp. Image Video Technol.* Cham, Switzerland: Springer, 2009, pp. 988–998.

[126] S.-J. Lin, "Fast-weighted secret image sharing," *Opt. Eng.*, vol. 48, no. 7, Jul. 2009, Art. no. 077008.

[127] P. Li, C.-N. Yang, C.-C. Wu, Q. Kong, and Y. Ma, "Essential secret image sharing scheme with different importance of shadows," *J. Vis. Commun. Image Represent.*, vol. 24, no. 7, pp. 1106–1114, Oct. 2013.

[128] P. Li, C.-N. Yang, and Z. Zhou, "Essential secret image sharing scheme with the same size of shadows," *Digit. Signal Process.*, vol. 50, pp. 51–60, Mar. 2016.

[129] C.-C. Chen, "Essential secret image sharing scheme with equal-sized shadows generation," *J. Vis. Commun. Image Represent.*, vol. 52, pp. 143–150, Apr. 2018.

[130] P. Li, Z. Liu, and C.-N. Yang, "A construction method of (t,k,n)-essential secret image sharing scheme," *Signal Process., Image Commun.*, vol. 65, pp. 210–220, Jan. 2018.

[131] M. K. Sardar and A. Adhikari, "Essential secret image sharing scheme with small and equal sized shadows," *Signal Process., Image Commun.*, vol. 87, Sep. 2020, Art. no. 115923.

[132] M. Yadav and R. Singh, "Essential secret image sharing approach with same size of meaningful shares," *Multimedia Tools Appl.*, vol. 81, no. 16, pp. 22677–22694, Jul. 2022.

[133] C.-C. Chen and S.-C. Chen, "Two-layered structure for optimally essential secret image sharing scheme," *J. Vis. Commun. Image Represent.*, vol. 38, pp. 595–601, Jul. 2016.

[134] C.-N. Yang and S.-M. Huang, "Constructions and properties of k out of n scalable secret image sharing," *Opt. Commun.*, vol. 283, no. 9, pp. 1750–1762, May 2010.

[135] Y.-Y. Lin and R.-Z. Wang, "Scalable secret image sharing with smaller shadow images," *IEEE Signal Process. Lett.*, vol. 17, no. 3, pp. 316–319, Mar. 2010.

[136] C.-N. Yang and Y.-Y. Chu, "A general (k, n) scalable secret image sharing scheme with the smooth scalability," *J. Syst. Softw.*, vol. 84, no. 10, pp. 1726–1733, Oct. 2011.

[137] Y.-X. Liu, C.-N. Yang, and P.-H. Yeh, "Reducing shadow size in smooth scalable secret image sharing," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2237–2244, Dec. 2014.

[138] Y. Liu and C. Yang, "Scalable secret image sharing scheme with essential shadows," *Signal Process., Image Commun.*, vol. 58, pp. 49–55, Oct. 2017.

[139] W. Liu, A. Wang, C.-C. Chang, Z. Li, and L. Liu, "A grouped-scalable secret image sharing scheme," *Multimedia Tools Appl.*, vol. 74, no. 17, pp. 7095–7109, Sep. 2015.

[140] Y.-C. Hou and Z.-Y. Quan, "Progressive visual cryptography with unexpanded shares," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1760–1764, Nov. 2011.

[141] C.-N. Yang, H.-W. Shih, C.-C. Wu, and L. Harn, "k out of n region incrementing scheme in visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 22, no. 5, pp. 799–810, Feb. 2011.

[142] C.-N. Yang, Y.-C. Lin, and C.-C. Wu, "Region-in-region incrementing visual cryptography scheme," in *Proc. Int. Workshop Digital Watermarking*. Cham, Switzerland: Springer, 2012, pp. 449–463.

[143] X. Yan, S. Wang, and X. Niu, "Threshold progressive visual cryptography construction with unexpanded shares," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8657–8674, Jul. 2016.

[144] S. Shivani and S. Agarwal, "Progressive visual cryptography with unexpanded meaningful shares," *ACM Trans. Multimedia Comput. Commun., Appl.*, vol. 12, no. 4, pp. 1–24, 2016.

[145] X. Yan and Y. Lu, "Progressive visual secret sharing for general access structure with multiple decryptions," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2653–2672, Jan. 2018.

[146] Y.-C. Chen, "Fully incrementing visual cryptography from a succinct non-monotonic structure," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1082–1091, May 2017.

[147] C.-N. Yang, C.-C. Wu, and Y.-C. Lin, "*k* out of *n* region-based progressive visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 1, pp. 252–262, Mar. 2017.

[148] Y.-X. Liu, C.-N. Yang, S.-Y. Wu, and Y.-S. Chou, "Progressive (k,n) secret image sharing schemes based on Boolean operations and covering codes," *Signal Process., Image Commun.*, vol. 66, pp. 77–86, Aug. 2018.

[149] H.-C. Chao and T.-Y. Fan, "Priority visual secret sharing of random grids for threshold access structures," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 11867–11882, May 2018.

[150] S. Sridhar and G. F. Sudha, "Quality improved (k, n) priority based progressive visual secret sharing," *Multimedia Tools Appl.*, vol. 79, pp. 1–28, May 2020.

[151] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theor. Comput. Sci.*, vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[152] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[153] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun. 2011.

[154] X. Yan, Y. Lu, and L. Liu, "General meaningful shadow construction in secret image sharing," *IEEE Access*, vol. 6, pp. 45246–45255, 2018.

[155] X. Yan, Y. Lu, L. Liu, and D. Ma, "Image secret sharing construction for general access structure with meaningful share," *Int. J. Digit. Crime Forensics*, vol. 10, no. 3, pp. 66–77, Jul. 2018.

[156] S. Shivani, "Multi secret sharing with unexpanded meaningful shares," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 6287–6310, Mar. 2018.

[157] R. De Prisco and A. De Santis, "Cheating immune (2,n)-threshold visual secret sharing," in *Proc. Int. Conf. Secur. Cryptogr. Netw.* Cham, Switzerland: Springer, 2006, pp. 216–228.

[158] Y.-C. Chen, D.-S. Tsai, and G. Horng, "A new authentication based cheating prevention scheme in Naor–Shamir's visual cryptography," *J. Vis. Commun. Image Represent.*, vol. 23, no. 8, pp. 1225–1233, Nov. 2012.

[159] J. Hartmanis, "Computers and intractability: A guide to the theory of NP-completeness (Michael R. Garey and David S. Johnson)," *SIAM Rev.*, vol. 24, no. 1, pp. 90–91, Jan. 1982.

[160] C.-C. Chang, C.-C. Lin, T. H. N. Le, and H. B. Le, "Sharing a verifiable secret image using two shadows," *Pattern Recognit.*, vol. 42, no. 11, pp. 3097–3114, Nov. 2009.

[161] Z. Eslami, S. H. Razzaghi, and J. Z. Ahmadabadi, "Secret image sharing based on cellular automata and steganography," *Pattern Recognit.*, vol. 43, no. 1, pp. 397–404, Jan. 2010.

[162] M. Ahmed and O. S. Younes, "Secret image sharing based on elementary cellular automata," in *Proc. Int. Conf. Adv. Intell. Syst. Inform.* Cham, Switzerland: Springer, 2017, pp. 832–843.

[163] X. Wu, D. Ou, Q. Liang, and W. Sun, "A user-friendly secret image sharing scheme with reversible steganography based on cellular automata," *J. Syst. Softw.*, vol. 85, no. 8, pp. 1852–1863, Aug. 2012.

[164] W.-T. Hu, M.-C. Li, C. Guo, and L.-F. Yuan, "A reversible steganography scheme of secret image sharing based on cellular automata and least significant bits construction," *Math. Problems Eng.*, vol. 2015, pp. 1–11, Jan. 2015.

[165] J. Zarepour-Ahmadabadi, M. Shiri-Ahmadabadi, and A. Latif, "A cellular automata-based multi-stage secret image sharing scheme," *Multimedia Tools Appl.*, vol. 77, no. 18, pp. 24073–24096, Sep. 2018.

[166] L. J. Anbarasi, G. S. A. Mala, and M. Narendra, "DNA based multi-secret image sharing," *Proc. Comput. Sci.*, vol. 46, pp. 1794–1801, Jan. 2015.

[167] C.-C. Yang, T.-Y. Chang, and M.-S. Hwang, "A (t,n) multi-secret sharing scheme," *Appl. Math. Comput.*, vol. 151, no. 2, pp. 483–490, 2004.

[168] T. Tuncer and E. Avci, "A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images," *Displays*, vol. 41, pp. 1–8, Jan. 2016.

[169] P. Eswaran and K. Shankar, "Multi secret image sharing scheme based on DNA cryptography with XOR," *Int. J. Pure Appl. Math.*, vol. 118, no. 7, pp. 393–398, 2017.

[170] A. G. Asuero, A. Sayago, and A. González, "The correlation coefficient: An overview," *Crit. Rev. Anal. Chem.*, vol. 36, no. 1, pp. 41–59, 2006.

[171] A. C. Sparavigna, "Entropy in image analysis," *Entropy*, vol. 21, no. 5, p. 502, May 2019.

[172] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption, cyber journals: Multidisciplinary journals in science and technology," *J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011.

[173] Y. A. Y. Ai-Najjar and D. C. Soong, "Comparison of image quality assessment: PSNR, HVS, SSIM, UIQI," *Int. J. Sci. Eng. Res.*, vol. 3, no. 8, pp. 1–5, Aug. 2012.

[174] Y.-W. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, and A. M. Barmawi, "Exploiting the error correction mechanism in QR codes for secret sharing," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Cham, Switzerland: Springer, 2016, pp. 409–425.

[175] J.-C. Chuang, Y.-C. Hu, and H.-J. Ko, "A novel secret sharing technique using QR code," *Int. J. Image Process.*, vol. 4, no. 5, pp. 468–475, 2010.

[176] S. Liu, Z. Fu, and B. Yu, "A two-level QR code scheme based on polynomial secret sharing," *Multimedia Tools Appl.*, vol. 78, no. 15, pp. 21291–21308, Aug. 2019.

[177] P.-C. Huang, C.-C. Chang, and Y.-H. Li, "Efficient (k,n)-threshold secret sharing method with cheater prevention for QR code application," *J. Internet Technol.*, vol. 23, no. 1, pp. 155–163, 2022.

[178] S. Wan, Y. Lu, X. Yan, and L. Liu, "Visual secret sharing scheme with (k, n) threshold based on QR codes," in *Proc. 12th Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, Dec. 2016, pp. 374–379.

[179] L. Tan, Y. Lu, X. Yan, L. Liu, and X. Zhou, "XOR-ED visual secret sharing scheme with robust and meaningful shadows based on QR codes," *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 5719–5741, Mar. 2020.

[180] H.-K. Tso and D.-C. Lou, "Medical image protection using secret sharing scheme," in *Proc. 6th Int. Conf. Ubiquitous Inf. Manage. Commun.*, Feb. 2012, pp. 1–4.

[181] A. Krishnan and M. L. Das, "Medical image security with cheater identification using secret sharing scheme," in *Proc. Int. Conf. Signal, Netw., Comput., Syst.* Cham, Switzerland: Springer, 2017, pp. 117–126.

[182] R. Basavegowda and S. Seenappa, "Electronic medical report security using visual secret sharing scheme," in *Proc. UKSim 15th Int. Conf. Comput. Model. Simul.*, Apr. 2013, pp. 78–83.

[183] A. Kanso and M. Ghebleh, "An efficient lossless secret sharing scheme for medical images," *J. Vis. Commun. Image Represent.*, vol. 56, pp. 245–255, Oct. 2018.

[184] A. Sarkar and M. Sarkar, "Tree parity machine guided patients' privileged based secure sharing of electronic medical record: Cybersecurity for telehealth during COVID-19," *Multimedia Tools Appl.*, vol. 80, no. 14, pp. 21899–21923, Jun. 2021.

SANCHITA SAHA (Member, IEEE) received the B.Tech. and M.Tech. degrees in CSE. She is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, Central Institute of Technology, Kokrajhar, Assam, India. She is currently an Assistant Professor with the Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia, West Bengal, India. She has a number of research publications in international journals and conference proceedings. Her research interests include information security and federated learning. She is a member of the Institution of Engineers, India.

ARUP KUMAR CHATTOPADHYAY (Member, IEEE) received the B.E. degree in computer science and engineering from SBMSIT (under Visvesvaraya Technological University), India, in 2002, the M.Tech. degree in computer science and application from A. K. Choudhury School of Information Technology (under the University of Calcutta), India, in 2011, and the Ph.D. degree from the Central Institute of Technology Kokrajhar, India. He is currently a Senior Teaching Fellow with the Indian Institute of Technology Madras, India. His research interests include cryptography and the Internet of Things.

ANUP KUMAR BARMAN (Member, IEEE) received the M.Sc., M.Tech., and Ph.D. degrees from Gauhati University, Assam. He is currently an Assistant Professor of computer science and engineering with the Central Institute of Technology Kokrajhar, Assam, India. He is actively engaged in a project called "CLIA-Cross-Lingual Information Access" executed in collaboration with various reputed institutes, such as Gauhati University, IIT Mumbai, IIT Hyderabad, and IIT Kharagpur. He is also engaged in various research activities, such as the development of the stemmer, word sense disambiguation module and parser, and so on for the Assamese language. He has more than 20 research publications in various international journals and conference proceedings. His research interests include natural language processing, machine learning, information retrieval, and information security.

AMITAVA NAG (Senior Member, IEEE) is currently a Professor of computer science and engineering with the Central Institute of Technology Kokrajhar, Assam, India. He has more than 50 research publications in various international journals and conference proceedings. His research interests include the IoT, information security, and machine learning. He is a fellow of IEI.

SUKUMAR NANDI (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology Kharagpur. He is a Professor with the Department of Computer Science and Engineering and the Head of the Centre for Linguistic Science and Technology at the Indian Institute of Technology Guwahati. He has more than 100 journal publications and several international conference publications. His areas of research interests include networks (specifically: QoS and wireless networks), computer and network security, data mining, VLSI, and computational linguistics. He is a fellow of the Indian National Academy of Engineering, a Senior Member of ACM, a fellow of the Institution of Engineers (India), and a fellow of the Institution of Electronics and Telecommunication Engineers (India).