IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 2 June 2024, accepted 4 July 2024, date of publication 11 July 2024, date of current version 29 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3426935

RESEARCH ARTICLE

Enhancing Healthcare Imaging Security: Color Secret Sharing Protocol for the Secure Transmission of Medical Images

SURESH SANKARANARAYANAN[1], (Senior Member, IEEE), PREMA BHUSHAN SAHANE[2], MAHESHWARI DIVATE[3], A. JOHN BLESSWIN[4], (Member, IEEE), G. SELVA MARY[4], (Member, IEEE), A. CATHERINE ESTHER KARUNYA[5], AND PASCAL LORENZ[6], (Senior Member, IEEE)

[1]Department of Computer Science, King Faisal University, Al Hofuf 31982, Saudi Arabia
[2]Department of Computer Engineering, JSPM's Rajarshi Shahu College of Engineering, Tathawade, Pimpri-Chinchwad 411033, India
[3]Department of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune 411018, India
[4]Directorate of Learning and Development, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, India
[5]School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, India
[6]Institute de Recherche en Informatique, Mathématique, Mathématiques, Automatique et Signal, University of Haute Alsace, 68000 Colmar, France

Corresponding authors: Suresh Sankaranarayanan (ssuresh@kfu.edu.sa), A. John Blesswin (johnb@srmist.edu.in), and G. Selva Mary (selvam1@srmist.edu.in)

This work was supported in part by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under Grant KFU241354.

ABSTRACT Healthcare has seen extensive use of internet technology for the transmission of electronic healthcare records among healthcare professionals and patients for diagnosis and treatment. Now with the advent of digital and internet technology, multimedia data also be transmitted in the form of images, and videos which include X-rays, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), and so forth. It is direly important to secure these medical images which are transmitted digitally among healthcare professionals and patients. Visual Cryptography (VC) comes as a solution for encrypting and securing these multimedia data for transmission. The process of VC involves dividing the original Secret Color Image into Shares and distributing them to the intended recipients. These shares are then combined, either physically or digitally, at the receiving end to reveal the original multimedia content. VC faces three main challenges which are the quality of reconstructed images, pixel expansion, and computational complexity. So, we in research developed a novel approach called Color Secret Sharing Protocol (CSSP) for the secure transmission of individual secret images within multimedia systems. The newly proposed protocol which is CSSP is been validated on sample medical images using MATLAB where the reconstructed image quality is improved by up to 1.345% compared to other existing methods. CSSP enhances multimedia security by utilizing cover images and simultaneously reducing complexity, effectively addressing pixel expansion within the context of multimedia transmission.

INDEX TERMS Cryptographic protocols, cryptography, electronic medical records, encryption, information security, medical information systems, visual communication.

I. INTRODUCTION

The healthcare applications have witnessed a remarkable transformation driven by integrating Internet technology into its core operations in recent years. The digitalization of healthcare records, Electronic Health Records (EHRs), and the seamless transmission of medical information have significantly enhanced the efficiency and accessibility of healthcare services. Notably, this technological shift has extended to medical imaging, where X-ray, CT, MRI, and other diagnostic

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

images are transmitted digitally in the format of Portable Network Graphics (PNG) and Joint Photographic Experts Group (JPEG), facilitating remote diagnosis and treatment planning. While this digitalization has brought tremendous advantages, it has also raised critical concerns about the security and privacy of sensitive medical images, especially concerning Patient Health Information (PHI). The protection of medical images is paramount due to the sensitive nature of their information. Patient privacy, confidentiality, and preventing unauthorized access are paramount to complying with stringent healthcare regulations and safeguarding patient trust. As medical images are increasingly exchanged among healthcare professionals and even directly with patients, ensuring their security during transmission becomes a pressing concern.

Information security encompasses the safeguarding of both textual and image data using information-hiding techniques, respectively. Steganography and watermarking are employed to conceal image data within Color Cover Images (I_{CC}), ensuring protection against copyright concerns. While cryptography serves as an effective encryption method for textual data, it becomes impractical for visual image data due to its large pixel count, resulting in laborious and costly encryption processes. To address this challenge, Naor and Shamir introduced Visual Cryptography (VC) as a means to encrypt images by dividing them into multiple shares. Shares individually do not expose Secret Color Image (I_{SC}), and the shares are stacked physically or digitally to reveal I_{SC} [1]. VC supports binary, grayscale, and color images and allows for the secure communication of multiple images [2]. VC finds application in binary, grayscale, and color images due to its effectiveness in both the encoding and decoding processes, which are commonly referred to as share construction and reconstruction phases, respectively. This technique proves to be advantageous in achieving efficient encoding and decoding of various image types. The initial application of VC involved binary images involving black and white and with two-layer transparencies. The usage of such advances includes grayscale and color images with multiple-layer transparencies [3], [4]. The VC technique incorporates security measures through the utilization of binary data. To enhance the cryptographic complexity, natural images are transformed into halftone images by adjusting the density of dots [5]. Initially, the physical stacking of the transparencies revealed the secret and later, digital stacking with XOR operations was done [13].

As the part of literature study, researchers have studied various methods to encrypt the image. In Binary image VC, an image has pixel values of either 0 or 255 that represent the colors black and white respectively. VC divides an image into n shares, and any k or n shares can reveal I_{SC}, resulting in a (k, n) or (n, n) scheme, respectively [1]. However, this method also leads to a pixel expansion problem, as the pixel values are encoded into multiple pixels. To address this pixel expansion issue, traditional VC shares are embedded with cover images I_{CC} to share images [6]. Researchers have proposed schemes to improve the performance of VC and reduce the complexity while reconstructing the images [17]. Upon the literature study carried out on various factors, the following are considered for this research work.

Pixel Expansion Factor: (i) The pixel expansion factor determines the size of the shares generated compared to the original secret image. Higher pixel expansion factors indicate larger shares. (ii) In the literature review, the pixel expansion factors vary across the different studies, ranging from 1 to n^2 *and* n^3 where n is a variable [9].

Number of Secret Images: (i) The number of secret images considered in the studies varies from 1 to multiple (n) secret images. (ii) Some studies focus on a single secret image, while others involve multiple secret images. (iii) The techniques used for generating shares may differ based on the number of secret images involved [7], [8].

Image Type: (i)The image format used in the studies is predominantly binary and grayscale, with some studies mentioning color image formats [12]. (ii) Color images provide richer visual information, allowing for more diverse and meaningful shares [11].

Types of Shares Generated: (i) Two main types of shares are mentioned: random shares and meaningful shares. (ii) Random shares are generated using randomization techniques, and halftoning techniques while meaningful shares preserve the visual content of the original image [10]. (iii) The choice of share type depends on the specific requirements and objectives of the visual cryptography scheme. Table 1 shows the important notations and the descriptions used in the proposed CSSP algorithm.

TABLE 1. Important notations used in the proposed CSSP.

Notation	Description
I_{SC}	Secret Color Image
I_{CC}	Color Cover Images
I_{Sh}	Share Images
I_{SI}	Semantic Images
th	Threshold value
$I_{SC_R}, I_{SC_G}, I_{SC_B}$	Secret Color Image of each channel Red, Green and Blue respectively
I_{RSC}	Reconstructed Secret Color Image
E_1, E_2, E_3	Encrypted Secret Pixel values
IE	Intermediate Encrypted Pixel
T	Temporary Pixel part
KP	Key Pixel
EF	Error Factor
SEF	Semantic Error Factor
RSEF	Reduced Semantic Error Factor
RBM	Random Binary Matrices

Based on the research objectives derived from a literature review of VC schemes, this research article proposes a new Colour Secret Sharing Protocol (CSSP). The objectives of the proposed CSSP scheme are to:

- transmit a single-color secret image I_{SC} securely from source to destination validated against attacks through histogram analysis and brute force testing.
- avoid pixel expansion issues in the share images compared with original secret image I_{SC} as measured by quantitative image analysis.
- enhance the quality of the reconstructed image and shares images to increase attack resilience and efficiency confirmed by image quality assessment and human evaluation.

The proposed algorithm securely communicates a single-color secret image using three color cover images $I_{CC1}, I_{CC2}, I_{CC3}$.

This research work focuses on constructing shares using a semantic pre-processed secret image without revealing any information about the original secret image. The construction of meaningful shares is achieved through simple calculations that are utilized during the process of revealing the secret. To enhance the quality of the Reconstructed Secret image, significant efforts are made to significantly reduce errors that may occur during the share construction and revealing phases [13], [14], [21]. The performance of the algorithm is measured using metrics such as Peak Signal-to-Noise Ratio (PSNR), Universal Image Quality Index (UIQI), Structural Similarity Index Measure (SSIM), and Mean Squared Error (MSE) [15]. After developing and testing the proposed algorithm using sample images, it was observed that the algorithm enhances the quality of the shares by up to 1.345% when compared to existing schemes. The research paper is structured as follows: Section II explains the proposed architecture's design, while Section III presents the implementation details and performance analysis of the proposed scheme. Section IV provides the conclusion and Future work.

II. PROPOSED ARCHITECTURE OF CSSP

The proposed CSSP aims to reduce pixel expansion, enhance security, improve the quality of Share Images (I_{Sh}), and reconstruct I_{SC} with minimal discrepancies. The scheme involves three key stages: Semantic Image Preparation, Share Generation, and Secret Image Reconstruction. The Semantic Image Preparation Stage assigns meaningful pixel and generates Semantic Images I_{SI} values to I_{SC}, ensuring content preservation during reconstruction. The Share Generation Stage divides I_{SC} into I_{Sh} and embeds them into I_{CC1}, I_{CC2}, *and* I_{CC3} to generate meaningful share images I_{SI1}, I_{SI2}, and I_{SI3}. Finally, the I_{SC} Reconstruction Stage retrieves the I_{Sh}, extracts the secret pixel values, and reconstructs the original secret image.

A. SEMANTIC IMAGE PREPARATION

The Semantic Image Preparation Stage is the initial phase in the CSSP. Its purpose is to process the I_{SC} and assign meaningful pixel values I_{SI1}, I_{SI2}, and I_{SI3}, ensuring that the reconstructed secret images have minimal pixel differences at the receiver end. During this stage, the I_{SC} is subjected to a transformation that involves calculating cumulative sums and deviation error factors for each pixel. This transformation helps in creating representations that preserve the visual content of I_{SC} while embedding them with meaningful characteristics. The representation of the semantic Image preparation process is depicted in Fig. 1.

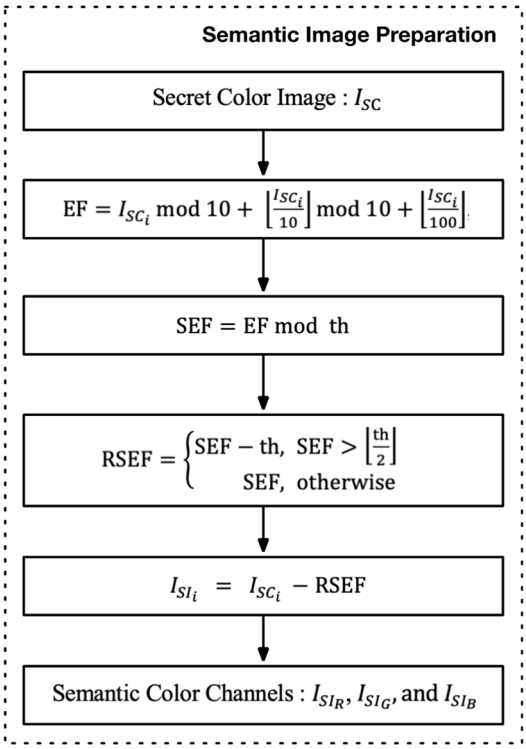


FIGURE 1. Semantic image preparation process.

The Semantic Image Preparation Stage involves the following steps:

Step 1: This stage takes the single-color image I_{SC} of size $H \times W$ as the input and separates its color channels Red (R), Green (G), and Blue(B). The dimensions represent the height (H), width (W). Create separate variables for each color channel $I_{SC_R}, I_{SC_G}, I_{SC_B}$. A color image of size $H \times W$ can also be represented as a three-dimensional array or matrix of size $H \times W \times 3$. Each element in this array corresponds to a pixel in the image and contains the color information for that pixel. The values in the array can range from 0 to 255, representing the intensity or color component for each channel.

Step 2: (0, 0) to (H, W) where $0 \leq H, W \leq 255$ each pixel is identified whether the particular pixel has semantic value or not. If not, the Error Factor (EF) and the Semantic Error Factor (SEF) are calculated using (1) ands (2). The th is the constant value assigned and is chosen as 9. The value is chosen to reduce the EF as low as possible so that the changes in the pixel value do not affect the image representation.

the selection of th in the proposed CSSP was a calculated decision based on empirical evidence and the theoretical underpinnings of our protocol's design. It ensures that the protocol effectively reduces the EF, maintains image quality, and is computationally efficient. The decision to use th also aligns with the digital encoding of images, where pixel values are typically manipulated within a base-10 system. mod10 is used to ensure that the transformed pixel values remain within the range of a single decimal digit, which is crucial for the encoding process within the proposed CSSP. This operation ensures pixel intensity values are restricted to the 0-9 range, which is pivotal for maintaining image quality and facilitating efficient encoding and decoding processes within the CSSP framework.

$$EF = I_{SC_i} mod 10 + \left\lfloor \frac{I_{SC_i}}{10} \right\rfloor mod 10 + \left\lfloor \frac{I_{SC_i}}{100} \right\rfloor,$$
$$i \in \{R, G, B\} \tag{1}$$

$$SEF = EF \ mod \ th \quad 0 \leq EF < th \tag{2}$$

In the operations involving fractional numbers and modular arithmetic, the floor function to the division result before the modulus operation is used. This method is consistent with conventional mathematical practices where fractional components are truncated to achieve integer-only results, thus preserving the integrity and correctness of the arithmetic processes involved. This practice ensures that our modular arithmetic operations are free from ambiguities and are correctly aligned with standard mathematical protocols.

Step 3: The error factor SEF needs to be reduced since the higher value of SEF can create a disturbance in the pixel value in the image. The Reduced Semantic Error Factor (RSEF) is calculated using (3).

$$RSEF = \begin{cases} SEF - th, & SEF > \left\lfloor \frac{th}{2} \right\rfloor \\ SEF, & otherwise \end{cases} \tag{3}$$

where the value ranges *between* $0 \leq \text{RSEF} < \lfloor \text{th}/2 \rfloor$

Step 4: The I_{SI_R}, I_{SI_G}, and I_{SI_B} are generated using (4).

$$I_{SI_i} = I_{SC_i} - RSEF, \quad \forall 0 \leq I_{SI_i} \leq ul \tag{4}$$

The upper limit for the pixel value is determined as ul, where *ul* is calculated as $255 - \lfloor \text{th}/2 \rfloor$).

B. SHARE GENERATION

Fig. 2 shows the Share generation stage of the proposed CSSP. I_{SC} is divided into I_{Sh}, and three cover images I_{CC1}, I_{CC2} and I_{CC3} are selected to embed the shared pixels and create meaningful I_{Sh}. Semantic color image generated from the previous stage in the form of Red (R), Green (G), and Blue (B) channels, with pixel values ranging from 0toul for each channel. I_{SC} is pre-processed to generate the semantic meaningful image $I_{SI1}, I_{SI2}, I_{SI3}$. A random binary matrix is generated to randomly separate the secret pixel values to the I_{Sh} so that enhanced security can be implemented. The transitional share pixels are chosen using RBM values and the $I_{CC1}, I_{CC2}, I_{CC3}$ are used as carriers so that meaningful I_{Sh} can be generated. The generated I_{Sh} looks very similar to the $I_{CC1}, I_{CC2}, I_{CC3}$. The $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are distributed to the participants of the communication through the communication channel.

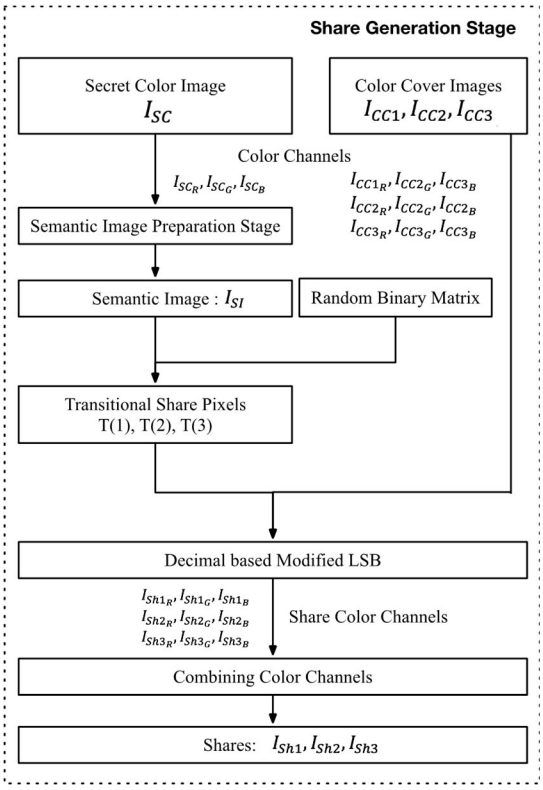


FIGURE 2. Share generation stage of the proposed CSSP.

The process of this stage is as follows:

Step 1: The resulting images $I_{SI_R}, I_{SI_G}, I_{SI_B}$ obtained from the previous stage is divided into transitional share pixels. Random Binary Matrices (RBM) of size $H \times W$ are generated using (5):

$$RBM_i = randi([0, 1], H, W), \text{ where } i \in \{R, G, B\} \tag{5}$$

Step 2: The share values are randomly selected from the transitional share pixels to enhance security. The selection of encrypted share values is determined using (6), (7), and (8):

$$T(1) = I_{SI_i} \ mod \ 10 \tag{6}$$

$$T(2) = \begin{cases} \left\lfloor \frac{I_{SI_i}}{10} \right\rfloor mod \ 10, & RBM_i = 1 \\ \left\lfloor \frac{I_{SI_i}}{100} \right\rfloor, & RBM_i = 0 \end{cases} \tag{7}$$

$$T(3) = RBM_i{}^{(x,y)} \tag{8}$$

where $i \in \{R, G, B\}$ and (x, y) are the pixel coordinates $0 \leq x, y \leq 255$.

This process is repeated for all three channels of the semantic secret color image. The resulting share values range from 0 to 9 and resemble binary images. However, sending such images may increase the likelihood of predicting the secret content. To enhance security, $I_{CC1}, I_{CC2}, I_{CC3}$ are utilized.

Step 3: The share values are embedded into the corresponding color $I_{CC1}, I_{CC2}, I_{CC3}$. The cover images $I_{CC1}, I_{CC2}, I_{CC3}$ are separated into their respective Red (R), Green (G), and Blue (B) channels. Each channel functions as an individual image, with pixel values ranging from 0 to 255. The encrypted share values obtained from Equations 6,7 and 8 are embedded into the cover channel images using the Decimal based Modified Least Significant Bit (DMLSB) embedding process [16], [17]. The proposed CSSP leverages the use of modulo 10 to encode numerical values within a single decimal digit, a technique that aligns with the base-10 encoding of the pixel intensity values commonly used in medical images. This method enables a one-to-one mapping of the pixel value adjustments to the 0-9 range, preserving the original image's visual and diagnostic integrity more effectively than binary LSB manipulation. The intermediate embedded $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are calculated using (9):

$$I_{Sh(Z)_i} = I_{CC(Z)_i} - I_{CC(Z)_i} mod 10 + T(Z) \tag{9}$$

where $i \in \{R, G, B\}$ and $\in \{1, 2, 3\}$

Step 4: The individual shares $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are communicated to the intended recipients through any open network channel. The $I_{Sh1}, I_{Sh2}, I_{Sh3}$ appear as color images that closely resemble the $I_{CC1}, I_{CC2}, I_{CC3}$ ensuring the confidentiality of the embedded secret information.

C. SHARE IMAGE RECONSTRUCTION

In the Secret Reconstruction Stage, the received shares $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are separated in to R, G, B channels. The DMLSB extraction method is utilized to extract values from each channel to reveal the secret pixel values [21]. The pixel values are decrypted by the following step-by-step process.

Fig. 3 shows that the shared images received from the participants are separated into color channels. The DMLSB extraction process extracts the secret encrypted pixel value. These values are random and are partial to get I_{SC} pixel. The values are used to generate a new Key Pixel (KP) value then the KP and the share values are used and digitally stacked together to get the original secret value.

If the $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are tampered or modified, KP from the share values would not be able to reveal the Reconstructed Secret Color Image (I_{RSC}). Also, without the reconstruction stage, I_{SC} will not be able to reconstruct I_{RSC} as it cannot be possible without the KP generated. This ensures the security of the $I_{Sh1}, I_{Sh2}, I_{Sh3}$ and I_{SC}.

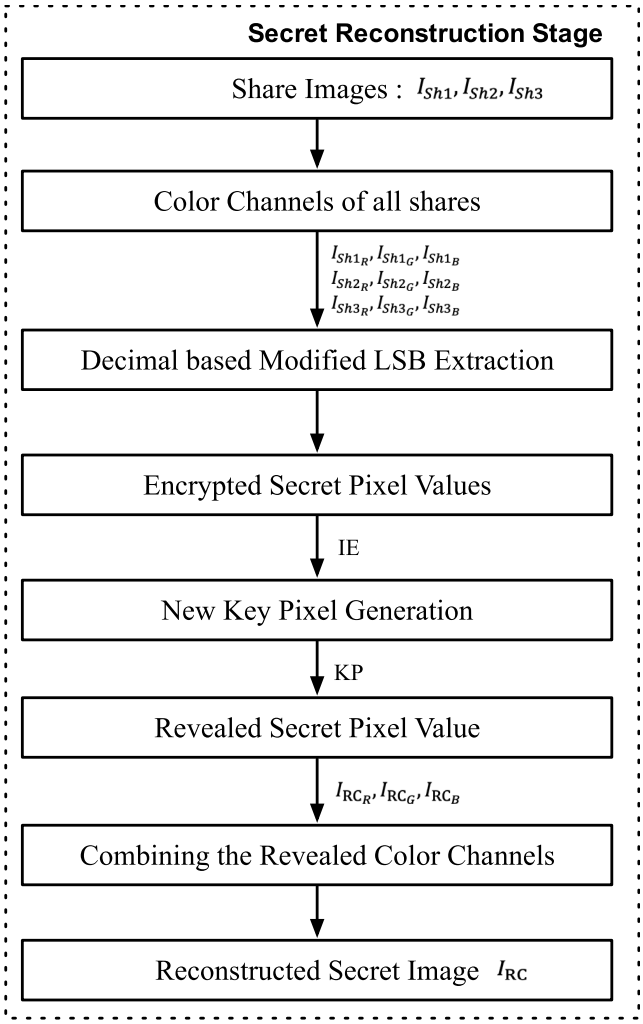


FIGURE 3. Secret image reconstruction stage of the proposed CSSP.

Step 1: $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are collected from the intended participants. The Encrypted Secret Pixel values E_1, E_2, E_3 are obtained from the I_{Sh1} by applying (10):

$$E_{(i,z)} = I_{Sh(z)_i} \; mod \; 10 \tag{10}$$

where $i \in \{R, G, B\}$ and $Z \in \{1, 2, 3\}$.

Step 2: The received encrypted secret pixel values are used to generate the missing KP values using (11) and (12):

$$IE_{(i)} = E_{(i,1)} + E_{(i,2)} \tag{11}$$

$$KP_{(i)} = \begin{cases} th - IE_{(i)}, & IE_{(i)} \leq th \\ 2 \times th - IE_{(i)}, & IE_{(i)} > th \\ 0 & IE_{(i)} = 0 \end{cases} \tag{12}$$

where th is a threshold value.

Step 3: The share values retrieved from the received $I_{Sh1}, I_{Sh2}, I_{Sh3}$ andKP are digitally stacked to obtain the secret

pixel values using (13):

$$I_{RSC(i)} = \begin{cases} KP_{(i)} \times 100 + E_{(i,2)} \times 10 + E_{(i,1)}, & E_{(i,3)} = 1 \\ E_{(i,2)} \times 100 + KP_{(i)} \times 10 + E_{(i,1)}, & E_{(i,3)} = 0 \\ 0 & otherwise \end{cases} \tag{13}$$

The procedure is repeated to the green and blue channels of all the $I_{Sh1}, I_{Sh2}, I_{Sh3}$ to retrieve the remaining secret image channels.

Step 4: All the reconstructed 3 channels are put together to reconstruct the Secret Color image I_{RSC} sent from the sender side.

The Channel representation of the Secret reconstruction phase for the red color channel is shown in Fig. 4.

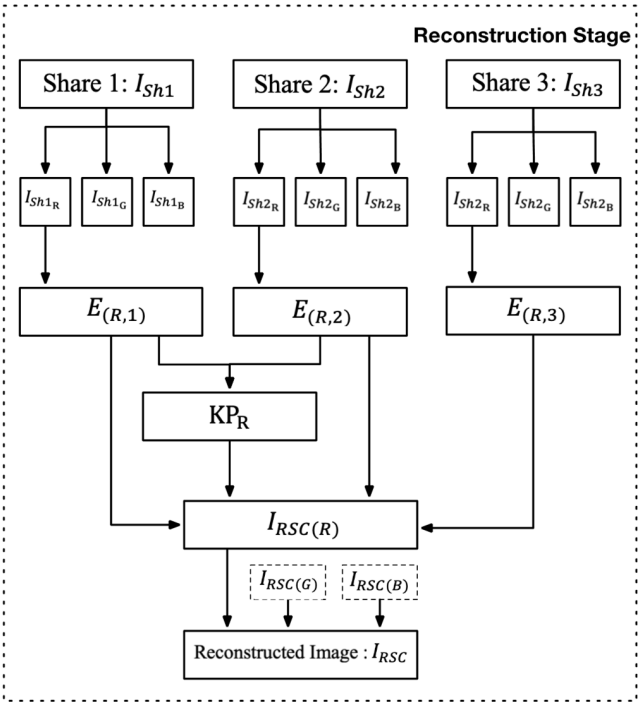


FIGURE 4. Channel-wise secret image reconstruction stage of the proposed CSSP.

In Fig. 4, the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, and the life cycle of each color channel in the reconstruction stage. Each color channel is used to reconstruct the key share KP and the secret. For the demonstration, only the process of red color channel is shown. In this section, the proposed CSSP is designed to securely communicate color secret images. The transmission ensures the confidentiality and security of the secret information.

In the Semantic Image Preparation Stage, the single-color secret image is processed to assign meaningful pixel values $I_{SI1}, I_{SI2}, I_{SI3}$. In the Share Generation Stage, the semantic images are divided into transitional share pixels. RBM are generated for each color channel. Encrypted share values are selected based on the transitional share pixels and the RBM to enhance the security of the pixel values. A minimum number of pixel values are sent to the receiver and the remaining pixel values are regenerated or recalculated at the receiving end. The algorithm for the Share Generation Stage is shown in Algorithm 1. The algorithm combines both the semantic image preparation and the share generation stage on the sender side.

In the Secret Reconstruction Stage, the received $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are separated into Red (R), Green (G), and Blue (B) channels. From the encrypted secret pixel values are extracted from the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, and missing KP values are generated. The secret pixel values are retrieved by stacking the share values using the obtained KP. This process is repeated for all channels of the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, and the reconstructed channels are combined to obtain the secret

Algorithm 1 Share Generation

Input: Single Color secret image I_{SC} and 3 color cover images $\{I_{CC1}, I_{CC2}, I_{CC3}\}$ of Size $H \times W$
Output: n Color share images $\{I_{Sh1}, I_{Sh2}, I_{Sh3} \ldots I_{Shn}\}$
begin :
Separate the color channels I_{SC_i} from $I_{SC}, i \in \{R, G, B\}$
Separate the color channels $I_{CC(Z)_i}$ from $I_{CC}, Z \in \{1, 2, 3\}$
For every i in I_{SC}:
For every $x \leftarrow 0 : H-1$
For every $y \leftarrow 0 : W-1$:

$$\mathrm{EF_i^{(x,y)}} = \mathrm{mod}\left(I_{SC_i}^{(x,y)}, 10\right) + \mathrm{mod}\left(\left\lfloor \frac{I_{SC_i}^{(x,y)}}{10} \right\rfloor, 10\right) + \left(\left\lfloor \frac{I_{SC_i}^{(x,y)}}{100} \right\rfloor\right)$$

$$\mathrm{SEF_i^{(x,y)}} = \mathrm{mod}\left(\mathrm{EF_i^{(x,y)}}, \mathrm{th}\right), 0 \leq \mathrm{SEF_i^{(x,y)}} < \mathrm{th}$$

$$\mathrm{RSEF_i^{(x,y)}} = \begin{cases} \mathrm{SEF_i^{(x,y)}} - \mathrm{th}, & \mathrm{SEF_i^{(x,y)}} > \left\lfloor \frac{\mathrm{th}}{2} \right\rfloor \\ \mathrm{SEF_i^{(x,y)}}, & \text{otherwise} \end{cases}$$

$$I_{SI_i}^{(x,y)} = I_{SC_i}^{(x,y)} - \mathrm{RSEF_i^{(x,y)}}$$

$$\forall 0 \leq I_{SI_i}^{(x,y)} \leq ul, ul = 255 - \left\lfloor \frac{\mathrm{th}}{2} \right\rfloor$$

Generate a random number r between 0 and 1

$$\mathrm{RBM_i^{(x,y)}} = \begin{cases} 0, & r \leq 0.5 \\ 1, & \text{otherwise} \end{cases}$$

$$\mathrm{T(1)_i^{(x,y)}} = \mathrm{mod}\left(I_{SI_i}^{(x,y)}, 10\right)$$

$$\mathrm{T(2)_i^{(x,y)}} = \begin{cases} \mathrm{mod}\left(\left\lfloor \frac{I_{SI_i}^{(x,y)}}{10} \right\rfloor, 10\right), & \mathrm{RBM_i^{(x,y)}} = 1 \\ \left\lfloor \frac{I_{SI_i}^{(x,y)}}{100} \right\rfloor, & \mathrm{RBM_i^{(x,y)}} = 0 \end{cases}$$

$$\mathrm{T(3)_i^{(x,y)}} = \mathrm{RBM_i^{(x,y)}}$$

Foreveery$Z \leftarrow 1 : 3$:

$$I_{Sh(Z)_i}^{(x,y)} = I_{CC(Z)_i}^{(x,y)} - \mathrm{mod}\left(I_{CC(Z)_i}^{(x,y)}, 10\right) + \mathrm{T(Z)_i^{(x,y)}}$$

end for
end for
end for
For every $Z \leftarrow 1 : 3$:
$I_{Sh(Z)}(:, :, 1) = I_{Sh(Z)_R}$
$I_{Sh(Z)}(:, :, 2) = I_{Sh(Z)_G}$
$I_{Sh(Z)}(:, :, 3) = I_{Sh(Z)_B}$
end for
end for
end begin

Algorithm 2 Secret Image Reconstruction

Input: Three color share images $\{SH_1, SH_2, SH_3\}$ of Size $H \times W$
Output: Reconstructed Secret Color image (RI_{SC})
begin :
Separate the color channels SH_{Z_i} from SH, $i \in \{R, G, B\}$, $Z \in \{1, 2, 3\}$
For every i in SH:
For every $x \leftarrow 0 : H-1$
For every $y \leftarrow 0 : W-1$:

$$E_{(i,1)}^{(x,y)} = \text{mod}\left(\text{SH}_{(\text{i},1)}^{(\text{x},\text{y})}, 10\right)$$
$$E_{(i,2)}^{(x,y)} = \text{mod}\left(\text{SH}_{(\text{i},2)}^{(\text{x},\text{y})}, 10\right)$$
$$E_{(i,3)}^{(x,y)} = \text{mod}\left(\text{SH}_{(\text{i},3)}^{(\text{x},\text{y})}, 10\right)$$
$$\text{IE}_{(\text{i})}^{(\text{x},\text{y})} = \text{E}_{(\text{i},1)}^{(\text{x},\text{y})} + \text{E}_{(\text{i},2)}^{(\text{x},\text{y})}$$
$$\text{KP}_{(\text{i})}^{(\text{x},\text{y})} = \begin{cases} \text{th} - \text{IE}_{(\text{i})}^{(\text{x},\text{y})}, & \text{IE}_{(\text{i})}^{(\text{x},\text{y})} \leq th \\ 2 \times \text{th} - \text{IE}_{(\text{i})}^{(\text{x},\text{y})}, & \text{IE}_{(\text{i})}^{(\text{x},\text{y})} > \text{th} \\ 0, & \text{IE}_{(\text{i})}^{(\text{x},\text{y})} = 0 \end{cases}$$
$$\text{RI}_{\text{SC(i)}} = \begin{cases} \text{KP}_{(\text{i})}^{(\text{x},\text{y})} \times 100 + E_{(i,2)}^{(x,y)} \times 10 + E_{(i,1)}^{(x,y)}, \\ \qquad E_{(i,3)}^{(x,y)} = 1 \\ E_{(i,2)}^{(x,y)} \times 100 + \text{KP}_{(\text{i})}^{(\text{x},\text{y})} \times 10 + E_{(i,1)}^{(x,y)}, \\ \qquad E_{(i,3)}^{(x,y)} = 0 \\ 0, \quad \text{otherwise} \end{cases}$$

end for
end for
For every $Z \leftarrow 1 : 3$:
$RI_{SC}(:, :, 1) = RI_{SC(R)}$
$RI_{SC}(:, :, 2) = RI_{SC(G)}$
$RI_{SC}(:, :, 3) = RI_{SC(B)}$
end for
end for
end begin

color image. Algorithm 2 shows the Secret Reconstruction phase receiving from the $I_{Sh1}, I_{Sh2}, I_{Sh3}$ at the receiver end to the decrypting of the image.

Through these stages, the CSSP ensures that the reconstructed secret images have minimal pixel differences compared to the original secret image. The scheme enables secure sharing and reconstruction of I_{SC} while preserving its visual content and minimizing discrepancies.

III. IMPLEMENTATION AND RESULT ANALYSIS

In this section, we focus on the implementation details and provide a comprehensive analysis of the results obtained from the Color Secret Sharing Scheme (CSSP). The CSSP algorithm was implemented using the MATLAB version R2020a tool, and a comprehensive evaluation was conducted using a set of color images as secret images [18], [19], [22]. The implementation involved utilizing various MATLAB functions and libraries to perform the necessary computations and image processing operations. The performance of the implemented CSSP algorithm was evaluated using several metrics, including Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), Universal Image Quality Index (UIQI), and Structural Similarity Index Measure (SSIM). These metrics were utilized to assess the visual quality, accuracy, and similarity between the original secret images and the reconstructed images generated by the algorithm [20], [22]. The analysis of these metrics provides valuable quantitative measures to evaluate the effectiveness and fidelity of the CSSP algorithm in preserving image quality and minimizing distortions during the sharing and reconstruction process.

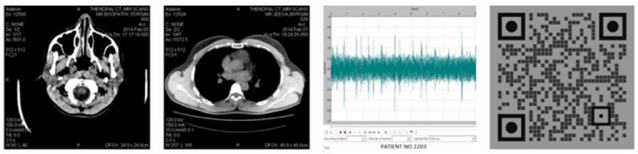
A. TOOLS USED

MATLAB version R2020a was chosen as the implementation tool for the CSSP algorithm due to several reasons. Firstly, MATLAB is a widely used programming environment that provides a comprehensive set of tools and functions for image processing and analysis. It offers a user-friendly interface and a rich library of built-in functions, making it convenient for implementing complex algorithms like CSSP. Furthermore, MATLAB provides extensive support for matrix operations, which is crucial for handling image data represented as matrices. This allows for efficient manipulation, transformation, and processing of the pixel values in the secret and $I_{CC1}, I_{CC2}, I_{CC3}$ during the different stages of the CSSP algorithm [23]. In addition, MATLAB offers various image processing and visualization functions that facilitate the analysis and evaluation of the algorithm's performance. It allows for easy calculation of metrics such as PSNR, MSE, UIQI, and SSIM, which are commonly used in image quality assessment. While MATLAB was a suitable choice for implementing the CSSP algorithm, there are alternative options available as well. Other programming languages like Python with libraries such as OpenCV or scikit-image could have been used. These languages also provide robust image-processing capabilities and have a large community of developers working on image-processing applications [24], [25], [26]. Additionally, specialized image processing software tools like ImageJ or Adobe Photoshop could have been utilized for implementing and evaluating the CSSP algorithm, although they might require additional customization and scripting capabilities [27]. Ultimately, the choice of implementation tool depends on factors such as familiarity, available resources, and specific requirements of the project. In this project, MATLAB is used for cost-effectiveness and the license version was available.

B. RESULT ANALYSIS

In this section implementation details provide a comprehensive analysis of the results obtained from the proposed CSSP. The CSSP algorithm was implemented using the MATLAB tool, and a comprehensive evaluation was conducted using a set of color images as secret images. After conducting the tests on the dataset, various metrics were computed and organized in a tabular format. These metrics provide insights into the performance of the CSSP algorithm, assessing factors

such as security, fidelity, and robustness. The sample secret images tested for this study are shown in Fig. 5.



(a) Secret image 1 (b) Secret image 2 (c) Secret image 3 (a) Secret image 4

FIGURE 5. Sample color secret test images.

Also, the sample MATLAB test colors $I_{CC1}, I_{CC2}, I_{CC3}$ are shown in Fig. 6.

(a) Cover Image 1 (b) Cover Image 1 (c) Cover Image 3

FIGURE 6. Sample color cover test images.

The entire lifecycle of I_{SC}, including the process of dividing it into $I_{Sh1}, I_{Sh2}, I_{Sh3}$ and reconstructing the original secret from the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, is visually depicted in Fig. 7.

Fig. 8 shows the matrix representation of the process of share generation for random pixel values. Four random matrices of size 4×4 has been taken as a red channel of a I_{SC}, I_{CC1}, I_{CC2}, and I_{CC3} pixel values respectively. The step-by-step transformation of pixel values is shown for demonstration purpose. RBM is the random matrix generated and the Share images $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are created.

1) SECURITY ANALYSIS

When analyzing the results of the CSSP algorithm in terms of security, several factors can be considered to evaluate the robustness of the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, and the confidentiality of I_{SC}. Here are some key aspects to measure the security including share correlation, share independence, and reconstruction accuracy. By considering reconstruction accuracy and conducting a comprehensive analysis, the security of the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, and I_{SC} regenerated by the CSSP algorithm is analyzed. It is important to strike a balance between security and the visual quality of the reconstructed secret image to ensure both confidentiality and usability. Reconstruction accuracy is measuring the accuracy of I_{SC} reconstruction process from the received $I_{Sh1}, I_{Sh2}, I_{Sh3}$. The $I_{Sh1}, I_{Sh2}, I_{Sh3}$ and I_{SC} are compared and the histogram analysis is shown in Fig. 9. For demonstration purposes, only the red channel of each of the image is compared.

When analyzing the histograms of the I_{Sh} and the I_{SC}, if they do not share a similar pattern, it suggests that the

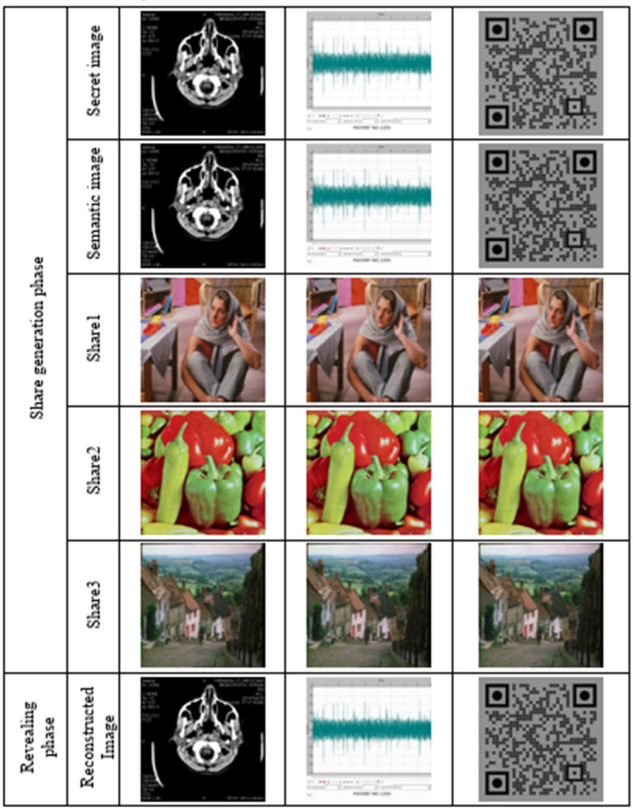


FIGURE 7. Lifecycle of secret test images of proposed CSSP.

I_{SC_R}

67	56	255	230
176	128	227	63
41	165	173	116
34	171	155	25

$I_{CC(1)_R}$

161	61	114	170
81	135	26	74
218	67	84	249
139	133	237	147

$I_{CC(2)_R}$

26	95	99	30
146	115	96	149
253	6	240	60
247	98	188	162

$I_{CC(3)_R}$

189	245	168	50
156	119	40	84
39	142	166	174
128	35	176	133

EF

13	11	12	5
14	11	11	9
5	12	11	8
7	9	11	7

SEF

4	2	3	5
5	2	2	0
5	3	2	8
7	0	2	7

RSEF

4	2	3	-4
-4	2	2	0
-4	3	2	-1
-2	0	2	-2

I_{SI_R}

63	54	252	234
180	126	225	63
45	162	171	117
36	171	153	27

RBM

0	1	0	0
1	1	1	1
1	1	0	1
1	0	1	1

T(1)

3	4	2	4
0	6	5	3
5	2	1	7
6	1	3	7

T(2)

0	5	2	2
8	2	2	6
4	6	1	1
3	1	5	2

T(3)

0	1	0	0
1	1	1	1
1	1	0	1
1	0	1	1

$I_{Sh(1)_R}$

163	64	112	174
80	136	25	73
215	62	81	247
136	131	233	147

$I_{Sh(2)_R}$

20	95	92	32
148	112	92	146
254	6	241	61
243	91	185	162

$I_{Sh(3)_R}$

180	241	160	50
151	111	41	81
31	141	160	171
121	30	171	131

FIGURE 8. Share generation stage for a 4 × 4 image.

distribution of pixel intensities in $I_{Sh1}, I_{Sh2}, I_{Sh3}$ does not provide direct information about I_{SC}. This is an important characteristic for security because it implies that an attacker who has access to individual $I_{Sh1}, I_{Sh2}, I_{Sh3}$ cannot gain any meaningful information about I_{SC} solely from its share. By keeping the histograms dissimilar, the scheme ensures

that no individual share reveals any visual or statistical characteristics of I_{SC}. This property enhances the security of the image-sharing scheme by preventing unauthorized users from extracting information about I_{SC} without the necessary $I_{Sh1}, I_{Sh2}, I_{Sh3}$. Therefore, when the histogram analysis demonstrates that the $I_{Sh1}, I_{Sh2}, I_{Sh3}$ do not share the pattern of I_{SC}, it indicates that the structure of the $I_{Sh1}, I_{Sh2}, I_{Sh3}$ successfully maintains the security of the image by preserving the confidentiality of the secret.

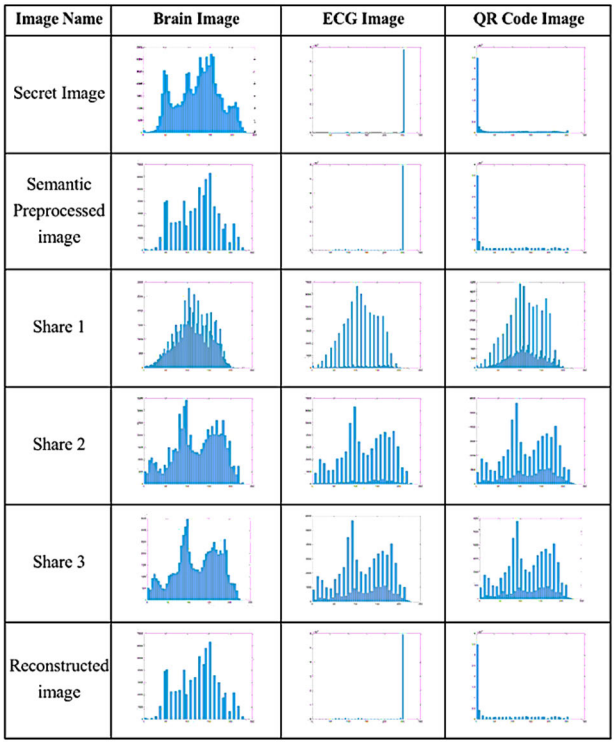


FIGURE 9. Histogram analysis of secret images.

Fig. 9 shows the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, and I_{SC} do not have any correlation and that does not give the chance of guessing the actual availability of secret inside the $I_{Sh1}, I_{Sh2}, I_{Sh3}$. Similarly, the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, and the reconstructed secret image do not have any resemblance. This protects I_{SC} from the share's extraction. Additionally, even with access to $I_{Sh1}, I_{Sh2}, I_{Sh3}$, an intruder cannot reconstruct the I_{RSC} without revealing the phase. The proposed schemes generate a new intermediate share during the revealing phase, which is essential for reconstructing the reconstructed secret image.

Enhanced Security Analysis on VC With Steganography:

Visual cryptography is an encryption technique that converts visual information into multiple shares. Each share is a random pattern of pixels, and when these shares are combined, the original image is revealed. One key advantage of visual cryptography is that the individual shares do not reveal any information about the original image.

In the proposed CSSP protocol, using VC, the original image I_{SC} is converted in to I_{SI} and the pixel values for example p(p1, p2, p3) of I_{SC} needs to be divided in to shares. The proposed CSSP uses a Random Binary Matrix (RBM) to generate shares by picking up $\{\langle(p1, p2) \mid (p2, p3) \mid p1, p3)\rangle\}$. In this process part of the p is used to generate the shares with the help of RBM. Each share is a separate image that appears random on its own but reveals the hidden data when combined with other shares. Each share generated by CSSP is embedded into different cover images using Decimal based Modified Least Significant Bit (DMLSB) steganography. This replaces the LSB from the pixel value in decimal number system. This technique modifies the LSBs of pixel values to hide share (the encrypted data), making the changes imperceptible to human eyes. Each share generated by CSSP's Share generation phase is embedded into different cover images. Fig. 10 shows the experimentation results while random LSB modification happens during attack in the share values. The share images without the LSB modification or removal are said to be true and all the shares without attack reveals the I_{RSC}. The received shares which were under attack are shown as *false* and during the decryption, the image is not reconstructed.

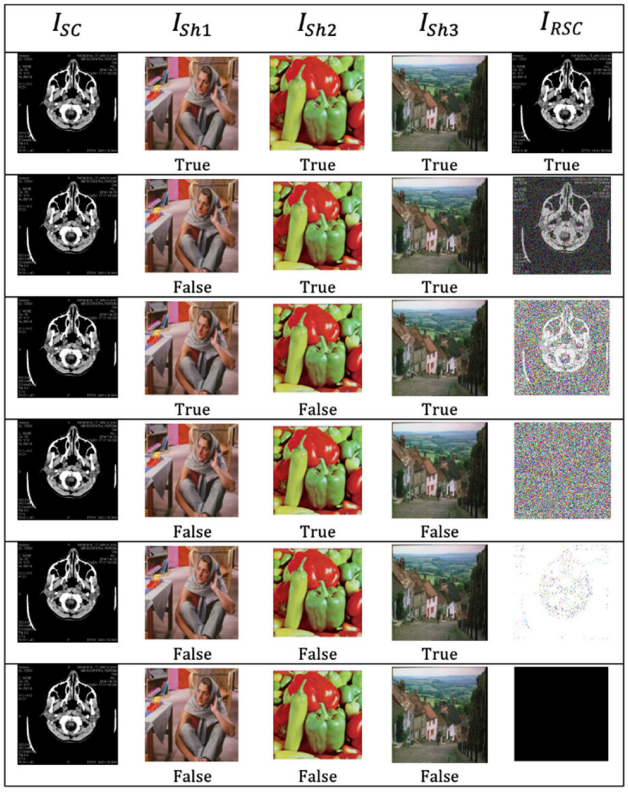


FIGURE 10. Robustness of proposed CSSP against LSB Removal or modification attack.

- Visual Cryptography Provides a robust layer of encryption. Each share is a random pattern and reveals no information about the original data independently. The shares are distributed across multiple cover images. An attacker would need to access all these images to reconstruct the original data. The original data be decrypted and visualized by combining all the shares.

- Even if an attacker detects the presence of hidden data, they cannot understand it without all the shares.
- VC shares are concealed within the cover images. The modifications to the LSBs are minimal, making it difficult for an attacker to detect the presence of hidden data.
- The visual quality of the cover images remains high and imperceptibility, as the changes are minor.
- The redundancy and partial distribution ensure that partial data remains meaningless and provides additional layer of security.

To demonstrate the robustness in our proposed CSSP, we conducted a comprehensive comparative analysis and robustness evaluation against various attack vectors:

Simple LSB Removal: The impact of removing the least significant bits from the share images is tested. If an attacker manages to detect hidden shares in some images, these values are random and are partial to get I_{SC} pixel. Even if the attacker manages to get all share values, the proposed CSSP's Share Image Reconstruction phase, uses the received encrypted share values to generate a new Key Pixel (KP) value matrix then the KP and the share values are digitally stacked together to get the original secret value. Without the reconstruction phase, the original image cannot be reconstructed.

Random LSB Modification: Evaluated the effect of randomly altering the LSBs. If the shares $I_{Sh1}, I_{Sh2}, I_{Sh3}$ are tampered or modified by the attacker, KP from the share values would not be able to reveal the I_{RSC}. It cannot be possible to generate the KP and the attacker cannot reveal the secret image. This ensures the security of the $I_{Sh1}, I_{Sh2}, I_{Sh3}$ and I_{SC}.

By combining visual cryptography with LSB steganography, we achieve a robust and secure method for hiding and protecting data. Visual cryptography provides strong encryption, making the data unreadable without all the shares, while LSB steganography ensures that the presence of hidden data is difficult to detect. This dual-layered approach significantly enhances the overall security of the hidden data.

To bolster the security of the proposed CSSP against well-known vulnerabilities, we have implemented multiple layers of defense as outlined below:

(i) Cheating Problem Mitigation: To address the risk of cheating, where fake shares might be introduced to produce an incorrect secret image, the proposed system will not be able to produce the I_{RSC}. These mechanisms are designed to detect the authenticity of shares prior to the reconstruction process, effectively preventing the acceptance of counterfeit shares.

Fig. 11 illustrates the process of verifying the authenticity and correctness of shares in case of cheating by one or more of the participants in the proposed CSSP and their impact on the reconstruction of the original secret image. The columns represent different shares and their reconstructions, labelled as $I_{SC}, I_{Sh1}, I_{Sh2}, I_{Sh3}$ and I_{RSC}. The rows correspond to various scenarios of share manipulation and reconstruction attempts.

Each cell contains an image and a label (for example TT, TF, FT, FF), indicating the authenticity and order correctness of each share:

- TT (True, True): The share is authentic and in the correct order. This scenario represents the ideal case where the share is genuine and held by the rightful owner. The reconstructed image is accurate (True).
- TF (True, False): The share is authentic but not in the correct order. Here, although the share is genuine, its disordering disrupts the reconstruction process, resulting in a flawed secret image.
- FT (False, True): The share is not authentic but is in the correct order. Even if the order is correct, the use of a fake share prevents successful decryption of the original secret.
- FF (False, False): The share is neither authentic nor in the correct order. This combination fails to reconstruct the original secret image.

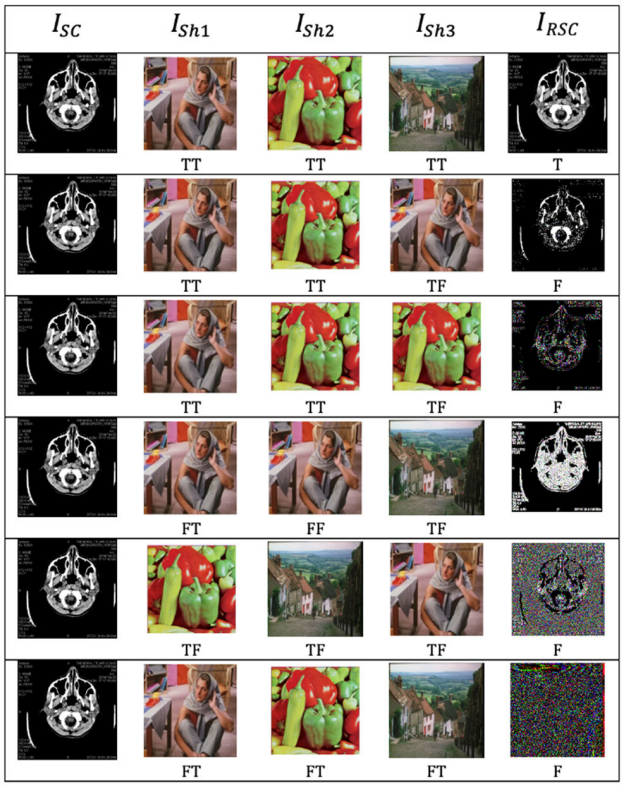


FIGURE 11. Robustness of proposed CSSP against cheating issues.

The labels TT, TF, FT, and FF indicate different scenarios in which participants might attempt to deceive the system. An authentic share submitted in the incorrect order (TF) or a fake share submitted in the correct order (FT) results in unsuccessful reconstruction of the secret image (False). In either case, the proposed CSSP ensures that the original secret cannot be decrypted, thereby maintaining the integrity and security of the visual cryptography system.

(ii) Man in the Middle (MitM) Attack Resistance: The proposed CSSP employs a sophisticated security strategy to resist MitM attacks effectively. This is achieved by encrypting pixel values using color transformations and modular arithmetic before decomposing these values into multiple units. Critically, only portions of these units are embedded into cover images during transmission, ensuring that no single share contains the complete information necessary to reconstruct the original image. This selective embedding significantly mitigates the risk of unauthorized reconstruction, as intercepting the shares alone does not provide the complete data needed.

During the revealing phase, CSSP's security is further reinforced as the remaining units of the encrypted data, not previously embedded, are recovered in a controlled environment. This phase requires that legitimate recipients possess the necessary cryptographic keys and knowledge of the protocol's operations, ensuring that even if an attacker accesses the shares, reconstruction of the image without the specific operations and keys from the revealing phase is infeasible.

The protocol's design incorporates randomness in the share generation phase, significantly enhancing security. Shares are created with a randomized distribution of encrypted pixel units, which prevents any predictable patterns that could be exploited by attackers. This randomness necessitates that an attacker must not only acquire all shares but also decipher the random distribution patterns used, a task that becomes exponentially more challenging with increased image size and complexity in share distribution. Fig. 10 and Fig. 11 provide empirical evidence supporting the robustness of the proposed CSSP against MitM attacks. The proposed CSSP's use of encryption, modular arithmetic, selective embedding, and randomization ensures robust protection against MitM attacks. By embedding only partial information in each share and requiring cryptographic keys for reconstruction, CSSP maintains the confidentiality and security of the secret image, even in the presence of interception attempts. These features are crucial for applications demanding high levels of security.

(iii) Brute Force Attack Resistance: In the scenario of a brute force attack, the complexity of guessing the correct pixel values is computationally impracticable. As the image size increases, the number of shares and the diversity of the embedding patterns also expand, necessitating that an attacker manage and decode a much larger volume of data. This scaling of attack complexity in proportion to image size and randomness introduces significant computational and knowledge barriers to unauthorized access. These barriers ensure that the CSSP not only secures the data during transmission but also systematically discourages and defeats attempts at unauthorized decryption, thus providing a robust framework for transmitting sensitive medical images. Given the pixel value range from 0 *to* 255 and the corresponding probabilities, the number of possible combinations for guessing even a single pixel is astronomically high, further exacerbated when considering multiple shares. This complexity ensures the impracticality of a brute force approach.

To illustrate the impracticality of a brute force attack, consider an image with width (W) and height (H) with 3 color channels namely Red, Green and Blue, where each pixel value ranges from 0 to 255. This image contains ($W \times H$) pixels, and for each pixel, three shares are generated. Let us consider a single-color channel Red.

Pixel Values and Shares: Each pixel can have one of 256 possible values (ranging from 0 to 255). For each pixel, 3 shares are generated, resulting in ($256^3 = 16,777,216$) possible combinations per pixel. Total Possible Combinations for the Entire Image is $W \times H$. Therefore, the total number of possible combinations for the entire image is $16,777,216^{W \times H}$.

Computational Feasibility: Assume an attacker has access to a supercomputer capable of testing 10^{12}(1 trillion) combinations per second. The expected time (T) to test all possible combinations is given by:

$$T = \frac{16,777,216^{W \times H}}{10^{12}}$$

$$T = \frac{2^{24^{W \times H}}}{10^{12}} \text{ as } 16,777,216 = 2^{24}$$

Therefore, the expected time T in seconds is $T = \frac{2^{24 \times (W \times H)}}{10^{12}}$

Conversion to Years: There are 31,536,000 seconds in a year, so the expected time in years is:

$$T = \frac{2^{24 \times (W \times H)}}{31,536,000 \times 10^{12}}$$

This results in an astronomically high number of years, far exceeding the age of the universe for any reasonable image size. This calculation clearly demonstrates that the time required to brute force an image of size $W \times H$ with 3 shares per pixel is impractically long, ensuring that the CSSP remains secure against such attacks. The above analysis considers only one-color channel (Red). For a full-color image with three channels (Red, Green, Blue), the complexity increases.

$$T = \frac{2^{24 \times 3 \times (W \times H)}}{31,536,000 \times 10^{12}} = \frac{2^{72 \times (W \times H)}}{31,536,000 \times 10^{12}}$$

This results in an even more astronomically high number of years, further demonstrating the impracticality of brute force attacks for full-color images.

The CSSP's design inherently scales the complexity of an attack in proportion to the image size and the randomness of share generation. As the image size increases, the number of shares and the diversity of the embedding patterns also expand, necessitating that an attacker manage and decode a significantly larger volume of data. This scaling of attack complexity introduces substantial computational and knowledge barriers to unauthorized access.

The CSSP's ability to resist brute force attacks is a testament to its robustness and effectiveness in ensuring data

security. The impracticality of brute force approaches further solidifies the protocol's capability to protect sensitive information against unauthorized access and decryption.

(iv) Mitigation of Accidental Attacks: The proposed CSSP is designed to be resilient not only to deliberate attacks but also to accidental noise or interferences that may introduce errors during the transmission of shares. This robustness is critical in ensuring the fidelity and integrity of the reconstructed image in a practical deployment. The proposed CSSP also accounts for accidental noise or interferences, which might introduce errors during transmission. In such events, key sharing process incorporates quality thresholds to identify when the reconstructed image's fidelity is compromised, prompting a retransmission request. The CSSP accounts for scenarios where accidental noise or interferences occur during the transmission of shares. These events might compromise the integrity of the shares and, consequently, the reconstructed image. Altered shares will disrupt the consistency of the pixel value reconstruction due to the cryptographic properties of the embedding and combining processes. If an authorized user changes any part of a share, this alteration will affect the encrypted pixel values distributed across the shares. Since the revealing phase relies on the correct alignment and combination of these values, any unauthorized change will result in incorrect or incomplete pixel reconstruction. This outcome is immediately noticeable and can trigger a re-verification or a request for retransmission of the original shares. Fig. 10 and Fig. 11 provide empirical evidence supporting the robustness of the proposed CSSP against accidental attacks. These features make CSSP robust against both external attacks and internal threats posed by authorized users attempting to manipulate the sharing process. Thus, the proposed CSSP is resilient to attacks and critical aspect of patient confidentiality and healthcare cybersecurity.

2) QUALITY ANALYSIS

The Quality of the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, and reconstructed image is an important factor while processing CSSP. A secure algorithm should achieve high reconstruction accuracy while maintaining the confidentiality of the secret information. The lower quality of the $I_{Sh1}, I_{Sh2}, I_{Sh3}$ may give security threats as it might provide the chances for the intruding agents to look for the secret inside it. If the quality is compromised at the receiving end, while reconstructing the secret, the purpose may get lost as it may not give the correct secret message.

a: MEAN SQUARE ERROR (MSE)

MSE, on the other hand, calculates the average squared difference between the pixel values of the original secret image and the reconstructed image. It provides a measure of the average distortion or error present in the reconstructed image. A lower MSE value indicates better image quality, as it signifies a smaller difference between the original and reconstructed pixel values. The error is given by (14)

$$MSE = \frac{\sum_{R,G,B} \sum_{x=1}^{H} \sum_{y=1}^{W} (I(x,y) - I'(x,y))^2}{3 \times H \times W} \quad (14)$$

Here, let I (x, y) be the original image and I′(x, y) be the decrypted image [23], [24], [25].

b: PEAK SIGNAL TO NOISE RATIO (PSNR)

PSNR serves as a metric assessing the relationship between the highest potential power of a signal and the disruptive noise. This metric gauge the quality of an image by analyzing the contrast between the initial secret image and the image after reconstruction. Higher PSNR values indicate better image quality, as it implies less distortion or noise in the reconstructed image [16], [26]. PSNR value is defined by (15).

$$PSNR = log \frac{(2^n - 1)^2}{MSE} \quad (15)$$

c: STRUCTURAL SIMILARITY INDEX (SSIM)

SSIM estimates the similarity between two images, depending on the initial uncompressed or bias-free image. SSIM is another widely used metric for assessing image quality. It measures the structural similarity between two images by considering the luminance, contrast, and structural information. SSIM considers the local variations in the images and provides a more accurate assessment of image similarity. Higher SSIM values indicate better image quality and a higher level of similarity between the original secret image and the reconstructed image [15], [27].

d: UNIVERSAL IMAGE QUALITY INDEX (UIQI)

UIQI is a perceptual quality metric that measures the similarity between two images based on their luminance, contrast, and structure. It considers factors such as mean luminance, standard deviation of luminance, and structural similarity. Higher UIQI values indicate better image quality, as it implies a higher level of similarity between the original secret image and the reconstructed image [23], [28], [29].

TABLE 2. Quality analysis of secret images vs. reconstructed images.

Metric	Secret Test Image 1	Secret Test Image 2	Secret Test Image 3
PSNR (dB)	40.865	39.145	41.286
MSE	0.5203	0.811	0.486
UIQI	0.9233	0.952	0.981
SSIM	0.9233	0.952	0.981
MAE	1.848	2.716	1.224

In the CSSP, the metrics such as PSNR, MSE, UIQI, and SSIM are calculated between the original secret image and the reconstructed image and are tabulated in Table 2. The analysis is shown in picture representation as in Fig. 12.

The quality analysis of cover images versus share images is essential to assess the impact of our visual cryptography

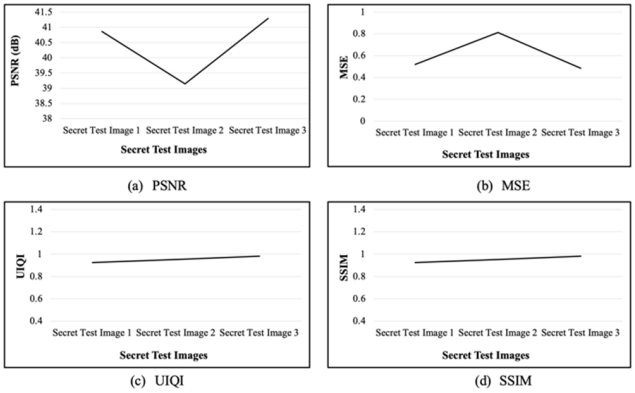


FIGURE 12. Quality analysis of secret test images of proposed CSSP.

techniques on image integrity and security. A robust visual cryptographic system should minimize the degradation of image quality, which helps prevent security risks that might arise from discernible changes visible to unauthorized parties. Significant changes in image quality could potentially reveal the presence of embedded data, compromising the confidentiality of the secret information. Table 3 shows to analyze the metrics for the cover and share images.

TABLE 3. Quality analysis of cover images vs. share images.

Metric	Share1 Vs Cover1	Share2 Vs Cover2	Share3 Vs Cover3
PSNR (dB)	39.32875	41.52133	40.40282
MSE	0.69347	0.38765	0.68018
MAE	2.39768	1.73145	2.39273
SSIM	0.85863	0.93672	0.86562

The quantitative analysis of image quality metrics between cover images and share images presents compelling evidence about the effectiveness after LSB embedding technique in visual cryptography. PSNR values indicate that the embedding process introduces minimal perceptible noise, suggesting a high retention of image quality. High PSNR values are typically indicative of less distortion, implying that the share images maintain a strong resemblance to their corresponding cover images. Lower MSE values denote smaller average differences between the pixel values of the original and embedded images, reinforcing the high fidelity of the reconstructed images. MAE scores further support the conclusion that the visual cryptography technique implemented does not significantly alter the visual content. Lower MAE values suggest that the average absolute deviation between the cover and share images is minimal, which is favorable for maintaining confidentiality and avoiding detection. The result shows the SSIM values close to 1 which are indicative of excellent image quality preservation. These metrics suggest that the structural integrity and visual quality of the images are well-preserved, maintaining both luminance and contrast fidelity post-embedding. The analysis reveals that the LSB embedding used in our visual cryptography scheme effectively disguises the secret data within the shares without significantly compromising image quality. This is crucial for ensuring that the presence of embedded data remains undetectable to unauthorized observers, thereby enhancing security. The high similarity and low error rates suggest that even if intercepted, the shares do not visually indicate the presence of embedded secrets, thus reducing the risk of targeted post LSB embedding attacks.

3) COMPARATIVE ANALYSIS

This section presents a comprehensive comparative analysis of the proposed Color Secret Sharing Protocol (CSSP) with state-of-the-art encryption methodologies, including AES Encryption, RSA Encryption, LSB Steganography, and DCT Steganography. Additionally, a detailed comparison with existing visual cryptography (VC) protocols is conducted, focusing on key performance metrics such as pixel expansion, security, quality, and computational complexity. This thorough evaluation aims to highlight the advantages of CSSP in providing enhanced security and reliability for sensitive biomedical applications.

(i) Proposed CSSP with Existing Encryption Methodologies: The security and integrity of biomedical images during transmission are paramount, necessitating robust encryption and steganography techniques. The comparison evaluates each method based on security, robustness, computational efficiency, and applicability to biomedical image transmission and shown in Table 4.

TABLE 4. Comparative study on proposed CSSP vs existing encryption methodologies.

Criteria	AES [32]	RSA [33]	LSB Steganography [34]	DCT Steganography [35]	Proposed CSSP
Security	High symmetric	High asymmetric	Low	Moderate	High combined
Brute Force	Highly resistant	Highly resistant	Low resistance	Moderate resistance	Highly resistant
MitM	Vulnerable without secure key exchange	Vulnerable without secure public key	Vulnerable	Moderately vulnerable	Highly resistant
Robustness	High	High	Low	Moderate	High
Noise Resistance	Sensitive to bit errors	Sensitive to bit errors	Very low	Moderate	High
Computational Efficiency	Fast	Slow	Very fast	Moderate	Fast
Suitability for images	Less	Less	Moderate	Moderate	Highly suitable

Advanced Encryption Standard (AES) is a symmetric key encryption algorithm providing high security and resistance to brute force attacks, though it can be vulnerable to MitM attacks if the key exchange process is not secure. AES ensures high robustness by encrypting the entire image, preserving its integrity but is sensitive to bit errors in the ciphertext.

It is known for its computational efficiency, offering fast encryption and decryption processes with hardware acceleration, making it highly suitable for biomedical image transmission [32].

Rivest, Shamir, Adleman (RSA), an asymmetric encryption algorithm, offers high security relying on the difficulty of factoring large numbers. It shares similar robustness to AES but is computationally intensive, making it slower and less practical for large image data. RSA is suitable for secure key exchange but less so for encrypting large files due to its computational demands [33], [34].

LSB Steganography embeds data into the least significant bits of pixel values, offering minimal security and low robustness, being easily affected by image compression and noise. It has very low computational overhead, making it efficient but less suitable for biomedical images due to its security vulnerabilities [35].

Discrete Cosine Transform (DCT) Steganography, embedding data in the frequency domain using Discrete Cosine Transform coefficients, provides better security than LSB with moderate resistance to noise and steganalysis attacks. It offers moderate robustness and computational complexity, making it more efficient than RSA but less so than LSB. DCT is moderately suitable for biomedical images, requiring careful implementation to avoid detection and ensure data integrity. In contrast, the proposed CSSP combines secret sharing with visual cryptography, offering high resistance to brute force and MitM attacks through encryption and selective embedding of pixel values. The proposed CSSP ensures high robustness due to its share verification mechanisms, preventing reconstruction errors caused by modifications or noise, and maintaining the integrity of the reconstructed image [36]. CSSP's computational efficiency is moderate to high, as the computations primarily involve basic arithmetic functions and modular operations, resulting in manageable computational overhead for enhanced security.

Designed to meet high security and integrity requirements, CSSP is highly suitable for biomedical image transmission, ensuring that the original secret cannot be decrypted if shares are manipulated or intercepted. The comparative analysis demonstrates that CSSP provides a robust and secure method for biomedical image transmission, surpassing traditional protocols such as AES and RSA in terms of security and robustness, while offering balanced computational efficiency and superior resistance to attacks, making it an ideal choice for sensitive biomedical applications.

(ii) Proposed CSSP with Existing VC Protocols: The proposed scheme is compared with other existing schemes and the results are tabulated in Table 5. The metrics are considered to analyze the quality performance. Based on the literature study and research work, a comparative analysis was conducted between existing visual cryptography (VC) schemes and the proposed VC schemes. The aim of developing the proposed protocols was to achieve specific research objectives such as pixel expansion, security, quality, and computational complexity [30]. Table 5 illustrates the results of the comparative analysis, highlighting the differences and similarities between the existing VC protocols and proposed protocols in relation to these objectives.

TABLE 5. Proposed vc protocols vs. existing protocols.

Type	Pixel expansion	Security	Quality	Decryption	Semantic Share	Shares	Image type
[1]	Yes	High	Low	Stack	No	n	Halftone
[6]	Yes	High	Low	Stack	No	n	Halftone
[7]	Yes	Medium	Medium	Stack	Yes	2	Halftone
[8]	Yes	High	Medium	Digital Stack	Yes	n	Halftone
[10]	Yes	High	Low	Stack	Yes	n	Halftone
[11]	No	High	Medium	Stack	Yes	2	Multitone
[15]	No	High	Medium	Digital Stack	No	n	Halftone
[16]	No	High	Low	Digital Stack	No	n	Halftone
[18]	No	High	Medium	Stack	No	2	Multitone
[21]	Yes	Medium	Medium	Stack	No	n	Halftone
[26]	No	High	Low	Digital Stack	No	2n	Multitone
Proposed CSSP	No	High	High	Digital Stack	Yes	3n	Multitone

This addition is aimed at offering readers a thorough understanding of the CSSP's operational efficiency and its practical applicability in real-world scenarios, where computational resources may be a constraint.

According to the findings presented, the proposed schemes outperform the existing schemes in terms of the research objectives. The proposed schemes demonstrate no pixel expansion in the reconstructed secret image. The size of the shared secret image and reconstructed remains the same. However, this does not compromise security. Moreover, the space complexity is effectively controlled as three shares can be used to send I_{SC}.

(iii) Complexity Analysis on Proposed CSSP with Existing VC Protocols: Table 6 outlines the computational complexity of the CSSP, detailing the algorithmic steps involved and quantifying their computational overhead. This analysis includes the time complexity of each stage of the protocol and the overall computational resources required for processing the encryption of secret images.

The $I_{Sh1}, I_{Sh2}, I_{Sh3}$ communicated through the channel do not reveal any information about the availability of secrets in the $I_{Sh1}, I_{Sh2}, I_{Sh3}$. Additionally, even with access to the $I_{Sh1}, I_{Sh2}, I_{Sh3}$, an intruder cannot reconstruct the I_{RSC} without revealing the phase. The proposed schemes generate a new intermediate share during the revealing phase, which is essential for reconstructing the reconstructed secret image. The quality of the reconstructed image is measured in terms of PSNR and MSE between I_{SC} and I_{RSC}. A higher PSNR

TABLE 6. Comparative study on complexity analysis.

Operations	Half-tone [3]	Semantic [23]	Significant [15]	Proposed CSSP
Addition	30 to 226	4	3	3
Division	5	2	2	3
Multiplication	7	2	2	0
Subtraction	Nil	1	1	4
Mod	Nil	2	2	4
Exec. Time (Sec)	2.9-6.8	0.5-1.12	0.181	0.128
Space Complexity	$7N^2$	N^2	N^2	N^2

value, typically between 30 and 50 dB, indicates better quality. The proposed schemes achieve PSNR values of more than 35 dB, ensuring that a good-quality reconstructed secret image is maintained. In summary, the comparative analysis reveals that the proposed schemes excel in achieving the research objectives of pixel expansion, security, quality, and complexity compared to the existing schemes.

IV. CONCLUSION AND FUTURE WORK

In this research paper, a new Color Secret Sharing Protocol (CSSP) has been proposed for the secure transmission of a single I_{SC}. CSSP enhances security by incorporating Color Cover Images I_{CC} into the sharing process. This addition helps to further protect the confidentiality of I_{SC}. One of the key advantages of CSSP is its ability to minimize complexity without introducing pixel expansion issues. This means that the original image's size remains intact, and there is no loss of quality during the sharing and reconstruction process. The proposed protocol also supports the sharing of multiple images, further expanding its practical applicability. By introducing CSSP, this research work contributes to the field of VC by providing a secure and efficient method for transmitting single secret color images. The incorporation of I_{CC} and the avoidance of pixel expansion issues ensure that the transmitted data remains confidential and of high quality. In summary, the proposed Color Secret Sharing Protocol offers an effective solution for securely transmitting single secret color images, addressing the security concerns associated with internet communication. Future research could focus on further enhancing the protocol's performance and extending its application to different types of multimedia data.

REFERENCES

[1] A. Arora, H. Garg, and S. Shivani, "Privacy protection of digital images using watermarking and QR code-based visual cryptography," *Adv. Multimedia*, vol. 2023, pp. 1–9, May 2023, doi: 10.1155/2023/6945340.
[2] M. Naor and A. Shamir, "Visual cryptography," *Adv. Cryptol.-Eurocrypt*, vol. 94, pp. 1–12, Jun. 1995.
[3] F. M. Aswad, I. Salman, and S. A. Mostafa, "An optimization of color halftone visual cryptography scheme based on bat algorithm," *J. Intell. Syst.*, vol. 30, no. 1, pp. 816–835, Jul. 2021, doi: 10.1515/jisys-2021-0042.
[4] Q. Wang, J. Blesswin A, T. Manoranjitham, P. Akilandeswari, S. Mary, S. Suryawanshi, and C. E. Karunya, "Securing image-based document transmission in logistics and supply chain management through cheating-resistant visual cryptographic protocols," *Math. Biosciences Eng.*, vol. 20, no. 11, pp. 19983–20001, Oct. 2023, doi: 10.3934/mbe.2023885.
[5] E. Çiftci and E. Sumer, "A novel steganography method for binary and color halftone images," *PeerJ Comput. Sci.*, vol. 8, p. 1062, Aug. 2022, doi: 10.7717/peerj-cs.1062.
[6] G. Selva Mary, A. J. Blesswin, and S. M. Kumar, "Self-authentication model to prevent cheating issues in grayscale visual secret sharing schemes," *Wireless Pers. Commun.*, vol. 125, no. 2, pp. 1695–1714, Jul. 2022, doi: 10.1007/s11277-022-09628-8.
[7] 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, doi: 10.1016/s0304-3975(99)00127-9.
[8] I. F. Elashry, O. S. Faragallah, A. M. Abbas, S. El-Rabaie, and F. E. A. El-Samie, "A new method for encrypting images with few details using rijndael and RC6 block ciphers in the electronic code book mode," *Inf. Secur. J., A Global Perspective*, vol. 21, no. 4, pp. 193–205, Jan. 2012, doi: 10.1080/19393555.2011.654319.
[9] S.-J. Lin and W.-H. Chung, "A probabilistic model of (T, N) visual cryptography scheme with dynamic group," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 197–207, Feb. 2012, doi: 10.1109/TIFS.2011.2167229.
[10] C.-C. Lin and W.-H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, nos. 1–3, pp. 349–358, Jan. 2003, doi: 10.1016/s0167-8655(02)00259-3.
[11] J. Blesswin and P. Visalakshi, "Optimal visual secret sharing on electrocardiography images for medical secret communications," *Int. J. Control Theory Appl.*, vol. 9, no. 2, pp. 1055–1062, 2016.
[12] J. Hao, H. Li, H. Yan, and J. Mou, "A new fractional chaotic system and its application in image encryption with DNA mutation," in *IEEE Access*, vol. 9, pp. 52364–52377, 2021, doi: 10.1109/ACCESS.2021.3069977.
[13] A. John Blesswin, G. Selva Mary, and S. Manoj Kumar, "Multiple secret image communication using visual cryptography," *Wireless Pers. Commun.*, vol. 122, no. 4, pp. 3085–3103, Feb. 2022, doi: 10.1007/s11277-021-09041-7.
[14] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009, doi: 10.1109/TIFS.2009.2024721.
[15] G. Selva Mary and S. Manoj Kumar, "Secure grayscale image communication using significant visual cryptography scheme in real time applications," *Multimedia Tools Appl.*, vol. 79, nos. 15–16, pp. 10363–10382, Apr. 2020, doi: 10.1007/s11042-019-7202-7.
[16] P. Puteaux, F. Yriarte, and W. Puech, "A secret JPEG image sharing method over GF(2M) Galois fields," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 6, pp. 3030–3042, Jun. 2022, doi: 10.1109/TCSVT.2022.3225644.
[17] J.-S. Pan, T. Liu, H.-M. Yang, B. Yan, S.-C. Chu, and T. Zhu, "Visual cryptography scheme for secret color images with color QR codes," *J. Vis. Commun. Image Represent.*, vol. 82, Jan. 2022, Art. no. 103405, doi: 10.1016/j.jvcir.2021.103405.
[18] 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, doi: 10.1109/TIFS.2018.2819125.
[19] Y. Guo, X. Jia, Q. Chu, and D. Wang, "A novel XOR-based threshold visual cryptography with adjustable pixel expansion," *Appl. Sci.*, vol. 10, no. 4, p. 1321, Feb. 2020, doi: 10.3390/app10041321.
[20] Y. Ren, F. Liu, T. Guo, R. Feng, and D. Lin, "Cheating prevention visual cryptography scheme using Latin square," *IET Inf. Secur.*, vol. 11, no. 4, pp. 211–219, Jul. 2017, doi: 10.1049/iet-ifs.2016.0126.
[21] G. Selva Mary and S. Manoj Kumar, "A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication," *Meas. Sci. Technol.*, vol. 30, no. 12, Dec. 2019, Art. no. 125404, doi: 10.1088/1361-6501/ab2faa.
[22] K. Patil, J. V. Barpute, M. Arkadi, D. Bhirud, C. Esther, J. Blesswin, S. Mary, and S. Raju, "Semantic pixel encoding visual secret sharing technique for balancing quality and security in color images," *J. Auto. Intell.*, vol. 7, no. 3, Jan. 2024, Art. no. 1159, doi: 10.32629/jai.v7i3.1159.
[23] C.-N. Yang, X. Wu, and M.-J. Chung, "Enhancement of information carrying and decoding for visual cryptography with error correction," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 20, no. 1, pp. 1–24, Jan. 2024, doi: 10.1145/3612927.
[24] D. Ibrahim, R. Sihwail, K. A. Z. Arrifin, A. Abuthawabeh, and M. Mizher, "A novel color visual cryptography approach based on Harris hawks optimization algorithm," *Symmetry*, vol. 15, no. 7, p. 1305, Jun. 2023, doi: 10.3390/sym15071305.

[25] N. Rani, S. R. Sharma, and V. Mishra, "Grayscale and colored image encryption model using a novel fused magic cube," *Nonlinear Dyn.*, vol. 108, no. 2, pp. 1773–1796, Apr. 2022, doi: 10.1007/s11071-022-07276-y.

[26] M. Z. Salim, A. J. Abboud, and R. Yildirim, "A visual cryptography-based watermarking approach for the detection and localization of image forgery," *Electronics*, vol. 11, no. 1, p. 136, Jan. 2022, doi: 10.3390/electronics11010136.

[27] A. Sherine, G. Peter, A. A. Stonier, K. Praghash, and V. Ganji, "CMY color spaced-based visual cryptography scheme for secret sharing of data," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–12, Mar. 2022, doi: 10.1155/2022/6040902.

[28] L. Wang, B. Yan, H.-M. Yang, and J.-S. Pan, "Flip extended visual cryptography for gray-scale and color cover images," *Symmetry*, vol. 13, Aug. 2020, Art. no. 65, doi: 10.3390/sym13010065.

[29] 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, doi: 10.1016/j.jvcir.2020.102793.

[30] C.-N. Yang, L.-Z. Sun, and S.-R. Cai, "Extended color visual cryptography for black and white secret image," *Theor. Comput. Sci.*, vol. 609, pp. 143–161, Jan. 2016, doi: 10.1016/j.tcs.2015.09.016.

[31] Handrizal, J. T. Tarigan, and D. I. Putra, "Implementation of steganography modified least significant bit using the columnar transposition cipher and Caesar cipher algorithm in image insertion," *J. Phys., Conf. Ser.*, vol. 1898, no. 1, Jun. 2021, Art. no. 012003.

[32] D. M. Alsaffar, A. S. Almutiri, B. Alqahtani, R. M. Alamri, H. F. Alqahtani, N. N. Alqahtani, G. M. alshammari, and A. A. Ali, "Image encryption based on AES and RSA algorithms," in *Proc. 3rd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Mar. 2020, pp. 1–5, doi: 10.1109/ICCAIS48893.2020.9096809.

[33] B. J. S. Kumar, V. K. Roshni Raj, and A. Nair, "Comparative study on AES and RSA algorithm for medical images," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2017, pp. 0501–0504.

[34] S. Rahman, J. Uddin, M. Zakarya, H. Hussain, A. A. Khan, A. Ahmed, and M. Haleem, "A comprehensive study of digital image steganographic techniques," *IEEE Access*, vol. 11, pp. 6770–6791, 2023, doi: 10.1109/ACCESS.2023.3237393.

[35] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A novel steganography technique for digital images using the least significant bit substitution method," *IEEE Access*, vol. 10, pp. 124053–124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

[36] Z. Zhu, N. Zheng, T. Qiao, and M. Xu, "Robust steganography by modifying sign of DCT coefficients," *IEEE Access*, vol. 7, pp. 168613–168628, 2019, doi: 10.1109/ACCESS.2019.2953504.

SURESH SANKARANARAYANAN (Senior Member, IEEE) is a Full Professor of computer science with the College of Computer Sciences and Information Technology, King Faisal University, Al Hofuf, Saudi Arabia. He has authored more than 100 international publications in refereed journals and conferences. He is a holder of five Indian patents and one U.S. patent to his credit in the field of the IoT, edge/fog computing, and artificial intelligence. His current Google Scholar citation is 2041 with an H-index of 22 and Scopus citation of 1047 with an H-index of 15. He has graduated five Ph.D.'s and more than 30 graduate research thesis and projects in the area of wireless sensors, the IoT, fog computing, intelligent agents, and machine learning. He has also been involved in lot of international collaborative project pertaining to the IoT, fog computing, and healthcare. His current research interests include the IoT, wireless sensor networks, Qos, edge computing, and machine learning. He is a reviewer and a technical committee member for a number of IEEE conferences and journals.

PREMA BHUSHAN SAHANE is currently pursuing the Ph.D. degree with Savitribai Phule Pune University. She is also an Assistant Professor with the JSPM's Rajarshi Shahu College of Engineering. With 17 years of comprehensive professional experience and boasting a rich academic background, she holds 11 years of expertise in teaching and an additional six years of hands-on industry experience. Her research endeavors are complemented by a prolific track record of patent filings, copyrights, and numerous publications in esteemed international and national journals and conference papers. Her multidimensional experience underscores her commitment to bridging the gap between academia and industry, contributing significantly to the scholarly discourse and technological advancements in her field.

MAHESHWARI DIVATE is currently pursuing the Ph.D. degree. She brings over a decade of dedicated experience in academia, prominently an Assistant Professor. She is with the Dr. D. Y. Patil Institute of Technology, Pune. She specializes in cloud computing, the IoT, and data visualization. Her core competency areas encompass cutting-edge technologies in the realm of information technology. As the Departmental Training and Placement Coordinator, she has played a crucial role in fostering institutional and administrative efficiency. Driven by a passion for education, she is committed to advancing knowledge and skill development in the field of engineering.

A. JOHN BLESSWIN (Member, IEEE) received the Master of Technology degree from Karunya University, India, and the Ph.D. from Anna University. He is an Associate Professor with over 14 years in academia, specializes in information communication engineering and web technologies. He has a prolific career, contributing to institutions, such as Anna University, SRM University, and Pune University, India. As a Leader of the DevOps Team, SRM University, he oversees processes and tool implementation and ensuring efficient software deployments. Committed to mentoring the next generation, he stays abreast of advancements in DevOps, cloud computing, and automation to enhance operational efficiency. He is guiding two Ph.D. research scholars and is also pursuing a Postdoctoral Fellowship with King Faisal University, Saudi Arabia. Passionate about integrating the latest tools, he ensures technological implementations align with institutional goals. Overall, he is a dynamic professional contributing significantly to the fields of academia, research, and technology. His research interests include visual cryptography, image security, web development, and teaching and learning methodologies.

G. SELVA MARY (Member, IEEE) received the Master of Engineering degree from the University of Mumbai and the Ph.D. degree from Anna University. She is an Assistant Professor with the Directorate of Learning and Development, SRM Institute of Science and Technology (SRMIST), Chennai, India. She is an accomplished academician with over 18 years of experience. Currently, she is the Head of eLearning technology with the SRMIST, a prestigious deemed-to-be-university in India, she is dedicated to transforming education through technology integration and innovative pedagogy. With a keen interest in staying abreast of industry advancements, she strives to incorporate the latest tools and practices, ensuring technological deployments align with institutional objectives. She is guiding three Ph.D. research scholars and is also pursuing a Postdoctoral fellowship with King Faisal University, Saudi Arabia. Overall, she is a dynamic researcher and an educator, committed to advancing the educational paradigm through technology and research. Her research interests include visual cryptography, image security, information communications, image communications, web development, and teaching and learning methodologies.

A. CATHERINE ESTHER KARUNYA is currently pursuing the Ph.D. degree (as a Research Scholar) with the SRM Institute of Science and Technology, Chennai, India. Reflecting her commitment to advancing knowledge in her chosen field. Simultaneously, she is currently Assistant Professor with the SNS College of Technology, Coimbatore, brings a wealth of expertise to the academic realm with a decade of dedicated service. Her scholarly pursuits are characterized by a keen interest in academia and her ten years of experience underscore her proficiency in pedagogy. Her research interests include visual cryptography, image communication, and information security, showcasing a specialized focus on cutting-edge technologies. Her research endeavors align with the ethos of continuous learning, and she is actively contributing to the academic landscape through her engagement in rigorous Ph.D. studies.

PASCAL LORENZ (Senior Member, IEEE) has been a Full Professor with the University of Haute Alsace, France, since 1995. He is the author/co-author of three books, three patents, and 200 international publications in refereed journals and conferences. His research interests include QoS, wireless networks, and high-speed networks. He is an IARIA Fellow and a member of many international program committees. He has organized many conferences, chaired several technical sessions, and gave tutorials at major international conferences. He is the Chair of IEEE ComSoc France (2014–2020), the Vertical Issues in Communication Systems Technical Committee Cluster (2008–2009), the Communications Systems Integration and Modeling Technical Committee (2003–2009), the Communications Software Technical Committee (2008–2010), and the Technical Committee on Information Infrastructure and Networking (2016–2017); and the Financial Chair of IEEE France (2017–2022). He has served as the Co-Program Chair for IEEE WCNC'2012 and ICC'2004; the Executive Vice-Chair for ICC'2017; the TPC Vice Chair for Globecom'2018; the Panel Sessions Co-Chair for Globecom'16; the Tutorial Chair for VTC'2013 Spring and WCNC'2010; the Track Chair for PIMRC'2012 and WCNC'2014; and the Symposium Co-Chair for Globecom 2007–2011, Globecom'2019, ICC 2008–2010, and ICC'2014 and '2016. He was a Technical Editor of *IEEE Communications Magazine* Editorial Board (2000–2006), *IEEE Networks Magazine* (since 2015), and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (since 2017). He has served as a Co-Guest Editor for special issues of *IEEE Communications Magazine*, *Networks Magazine*, *Wireless Communications Magazine*, *Telecommunications Systems*, and LNCS. He is an Associate Editor of *International Journal of Communication Systems* (IJCS-Wiley), *Journal on Security and Communication Networks* (SCN-Wiley), and *International Journal of Business Data Communications and Networking*, and *Journal of Network and Computer Applications* (JNCA-Elsevier). He was an IEEE ComSoc Distinguished Lecturer Tour from 2013 to 2014.