

## ORIGINAL RESEARCH ARTICLE

# Semantic pixel encoding visual secret sharing technique for balancing quality and security in color images

Kanchan Patil<sup>1</sup>, Jyotsna Vilas Barpute<sup>2</sup>, Mrudul Arkadi<sup>3</sup>, Sapana Deepak Bhirud<sup>4</sup>, Catherine Esther Karunya A<sup>5</sup>, John Blesswin A<sup>6,\*</sup>, Selva Mary G<sup>6,\*</sup>, Shibani Raju S<sup>7</sup>

<sup>1</sup> Department of Information Technology, SRES's Sanjivani College of Engineering, Kopargaon (MH) 423603, India

<sup>2</sup> Department of Artificial Intelligence and Data Science, Dr.D.Y.Patil Institute of Technology, Pimpri 411018, India

<sup>3</sup> Department of Information Technology, Don Bosco institute of Technology, Kurla, Mumbai 400070, India

<sup>4</sup> Department of Artificial Intelligence and Machine Learning, PES Modern college of engineering, Shivajinagar, Pune 411005, India

<sup>5</sup> School of Computing, SRM Institute of Science and Technology, Kattankulathur 603203, India

<sup>6</sup> Directorate of Learning and Development, SRM Institute of Science and Technology, Kattankulathur 603203, India

<sup>7</sup> Department of Computer Science and Engineering, Madras Institute of Technology, Chennai 600025, India

\* **Corresponding authors:** John Blesswin A, johnblesswin.rnd@gmail.com; Selva Mary G, selvamaryg.rnd@gmail.com

## ABSTRACT

Color images are widely utilized across various domains, encompassing digital media and extending to critical applications in satellite and military arenas. As the significance of these images has grown, the need to protect their content from unauthorized access and potential threats has been underscored. Visual Secret Sharing (VSS) schemes have been proposed as effective mechanisms, with images being encrypted into multiple shares that, individually, offer no discernible information about the original content. Nevertheless, issues such as pixel expansion have been noted in traditional VSS methods, which result in increased complexity and a potential compromise in image quality. Maintaining impeccable image quality is emphasized, mainly since critical application decisions are often based on the clarity and accuracy of image details. The Semantic Pixel Encoding Visual Secret Sharing (SPEVSS) technique is proposed to address these identified challenges. A robust mechanism has been formulated through the integration of semantic pixel encoding with VSS, effectively countering pixel expansion while preserving the fidelity of the original image. As a result of this research, computational complexity has been significantly reduced, decryption methodologies have been made more efficient, and a more robust security framework for colour images has been established. The performance of the proposed SPEVSS shows the reconstructed images show the PSNR of 42 dB has been recorded in images processed, underscoring the method's capability to balance security and optimal image quality.

**Keywords:** semantic images; visual secret sharing; color visual cryptography; pixel encoding

## ARTICLE INFO

Received: 18 August 2023  
Accepted: 30 October 2023  
Available online: 4 January 2024

## COPYRIGHT

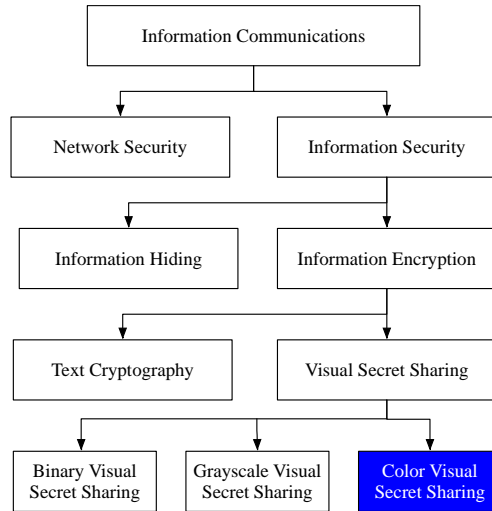
Copyright © 2024 by author(s).  
Journal of Autonomous Intelligence is published by Frontier Scientific Publishing. This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).  
<https://creativecommons.org/licenses/by-nc/4.0/>

## 1. Introduction

In an era of digital communication, the importance of information security has never been more pronounced. Color images, with their rich data and visual content, have emerged as integral mediums for conveying information across various domains. These images are widely utilized, from digital media landscapes to more specialized arenas like satellite imaging and military operations. As communication intensifies, particularly between critical infrastructures, the need for stringent security measures becomes paramount. The transmission of sensitive satellite images, vital for surveillance,

mapping, and defence strategies, as well as military communications, pivotal for operational success, underscores the gravity of this need.

**Figure 1** provides a taxonomy view of the solutions in image security. At its core, the flowchart delineates the bifurcation between network-level security, which focuses on the transmission infrastructure, and information security, which prioritizes the communication content. Within information security, encryption emerges as a primary defence mechanism. While text-based encryption has its merits, the unique nature of visual data demands specialized solutions.



**Figure 1.** Taxonomy of visual secret sharing.

Visual Secret Sharing (VSS) or Visual Cryptography (VC) is a technique tailored for images. VC stands out by splitting an image into multiple shares or shadows, ensuring that only a collective combination reveals the original content. However, VC's pioneering approach has its pitfalls. Issues such as pixel expansion can complicate the encryption process, potentially compromising image quality—a concern becomes magnified when considering the stakes in satellite and military applications. The shares or shadows shared are in binary color with black and white dots in the image in the traditional methods. This makes the chance for the intruder to guess the presence of Secret in the image. Hence, it is important to create semantic image with meaning to the share by encrypting the share image to the cover image. This cover image and the share images are not only providing semantic representation to the share but also need the decryption algorithm to reveal the secret image. The Semantic Pixel Encoding Visual Secret Sharing (SPEVSS) technique, is proposed as a solution to these challenges. By integrating semantic pixel encoding with traditional VC principles, SPEVSS promises to mitigate pixel expansion issues and restore decrypted images to their original quality.

## 2. Review of literature work

The significance of safeguarding visual information, particularly color images, has been underscored in the recent literature. With the proliferation of digital media and critical applications spanning satellite and military domains, ensuring the confidentiality, integrity, and authenticity of color images during communication has become paramount. VSS is characterized by its capability to encrypt visual data so that decryption doesn't necessitate complex computations. Introduced as a foundational concept, VC enabled decomposing a secret image into multiple shares without revealing significant information about the original image in individual shares<sup>[1]</sup>. A comprehensive overview of VSS techniques highlighted the nuances and advancements over the years, encapsulating the growth and evolving challenges in the field<sup>[2]</sup>. With the proliferation of digital media and multimedia communications, ensuring the security of color images has become paramount. A study delved into the combined utility of watermarking and QR Code-based VSS to

enhance the privacy protection of digital images, showcasing the interplay between traditional and novel cryptographic mechanisms for digital images<sup>[3]</sup>. Expanding the horizons of VC, a notable approach integrated error diffusion in colour-extended VSS, significantly improving the fidelity of the reconstructed secret colour images<sup>[4]</sup>.

Further exploration in the domain of colour VC focused on the encryption of black-and-white secret images, using a methodology that hinges on extended colour VSS, paving the way for more versatile applications<sup>[5,6]</sup>. The journey of VC is not without its challenges. Issues such as pixel expansion, poor decryption quality, and increased computational complexity have been persistent concerns in the domain. An optimized color halftone VSS scheme leverages a unique algorithm to overcome these inherent problems<sup>[7]</sup>. A significant VSS scheme was introduced specifically tailored underscoring the importance of adapting VC techniques to various image types and application scenarios<sup>[8]</sup>. Innovations in VC have often sought inspiration from nature. A recent study presented a novel approach to colour VC, showcasing the potential of bio-inspired techniques in enhancing VC methodologies<sup>[9]</sup>. The significance of VC extends to specialized fields like healthcare. A proposed unique privacy protection framework for medical image security combines VSS with another method, ensuring that medical images remain secure without relying on traditional cryptographic keys<sup>[10]</sup>. Ensuring the authenticity of decrypted images is as crucial as their encryption. A study introduced a self-authentication model for understanding the cheating issues, emphasizing the importance of trustworthiness in the decrypted outputs<sup>[11]</sup>. Steganography, the art of concealing information within other information, has found its synergy with VC. A novel steganography method was introduced showcasing the potential of combining steganographic techniques with VC for enhanced image security<sup>[11]</sup>. The reviewed literature underscores the dynamism and evolving nature of VSS. From foundational principles to nature-inspired algorithms, the field has witnessed myriad innovations to enhance the security and fidelity of encrypted images. As digital communication continues to grow, ensuring visual data security remains paramount, making the advancements in VC crucial for future multimedia communications.

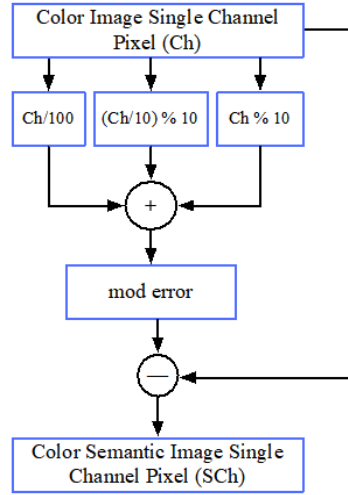
The objectives of this research are clear: to refine and enhance the VC process, ensuring optimal security without compromising image fidelity. As outlined in the abstract, the anticipated outcomes speak to a future where color images, irrespective of their application, can be transmitted with confidence in their security and quality.

### 3. Proposed methodology

The proposed Semantic Pixel Encoding Visual Secret Sharing (SPEVSS) consists of three stages namely, Semantic Pixel Generation, Pixel Encoding and Share Generation stage and Pixel Reconstruction stage.

#### 3.1. Semantic pixel generation

**Figure 2** shows the process of transforming a secret color image *SCI* into its semantic counterpart, denoted as *SSCI*. During this transformation, pixels are rendered meaningful through specific pixel values, resulting in a semantic image whose pixel values span a range from  $SSCI \in \{0, 1, 2, \dots, 252\}$ . A distinctive feature of the semantic image is its discrete pixel values, which often resemble those of neighbouring pixels, thereby giving rise to pixel clusters. The process to achieve this transformation, as illustrated in **Figure 2**, unfolds as follows:



**Figure 2.** Semantic pixel generation.

To commence, the secret color image undergoes a separation into its three primary channels: Red, Green, and Blue. Each of these channels encompasses pixel values that range between 0 and 255. The proposed SPEVSS approach treats each channel independently, subjecting every pixel within each channel to a series of steps to achieve its semantic representation:

---

**Algorithm 1** Generation of Semantic Pixel

---

- 1: *Input:  $SCI^{RGB}$  of size  $X \times Y$  of RGB channels - Secret color Image*
  - 2:  $SCI^R, SCI^G, SCI^B \leftarrow RGB \leftarrow SCI^{RGB}$
  - 3: *Output:  $SSCI^{RGB}$  of size  $X \times Y$  of RGB channels - Semantic Secret Color Image*
  - 4: *For each channel R, G, B of SCI,*
  - 5: *For each m: 1 to X*
  - 6: *For each n: 1 to Y*
  - 7: *while(m,n)*
  - 8:  $Error_{m,n} \leftarrow \left( (SCI_{m,n} \% 10) + \left( \frac{SCI_{m,n}}{10} \% 10 \right) + \frac{SCI_{m,n}}{100} \right)$
  - 9:  $Error'_{m,n} \leftarrow Error_{m,n} \bmod error$
  - 10:  $SSCI_{m,n}^R \leftarrow SCI_{m,n}^R - Error'_{m,n}$
  - 11:  $SSCI_{m,n}^G \leftarrow SCI_{m,n}^G - Error'_{m,n}$
  - 12:  $SSCI_{m,n}^B \leftarrow SCI_{m,n}^B - Error'_{m,n}$
  - 13:  $SSCI^{RGB} \leftarrow RGB(SCI^R, SCI^G, SCI^B)$
- 

Algorithm 1 shows the sequential procedure to generate a  $SSCI$  from the  $SCI$ .

**Step 1:** Initiate by computing the error associated with each pixel. This computation aids in deriving the integer coefficients of the pixel.

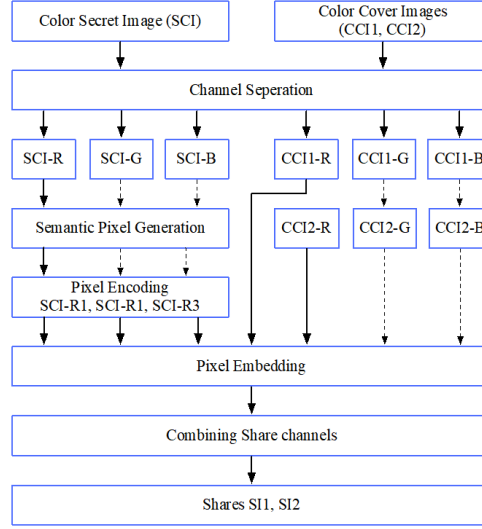
**Step 2:** The construction of the  $SSCI$  is accomplished by attenuating these pixel errors. Every pixel's Pixel Error ( $e$ ) is ascertained and subsequently subtracted from its original pixel values, as elaborated in<sup>[12,13]</sup>. By doing so, pixels are endowed with a more meaningful representation. It's pertinent to note that any error's threshold value ( $e$ ) is set at 9.

**Step 3:** In the SPEVSS method proposed, the value of ( $error$ ) undergoes further reduction.

**Step 4:** The act of subtracting this diminished error from the original pixel yields a pixel with enhanced meaning. This procedure not only preserves but also enhances the quality of the resulting semantic image.

### 3.2. Pixel encoding and share generation stage

In this section, we detail the steps of the sharing and embedding phase, also known as the share construction phase. **Figure 3** provides a visual guide to this phase. Here, the secret color image SCI is split into its primary Red (SCI-R), Green (SCI-G), and Blue (SCI-B) channels.



**Figure 3.** Pixel encoding and share generation.

The color channels are taken from the main secret image SCI for this process. Next, the semantic image is created using the method in Algorithm 1. The steps to make the shares are presented in Algorithm 2.

---

**Algorithm 2** Pixel Encoding and Share generation algorithm

---

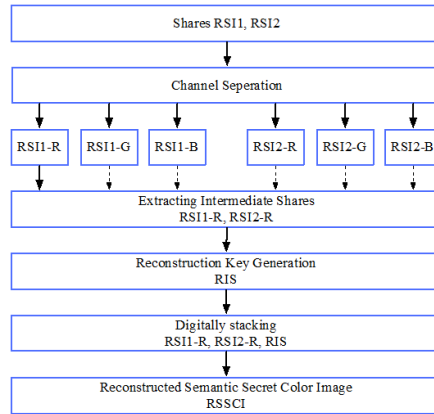
- 1: Input:  $SCI^{RGB}, CC^1, CC^2, CC^3$  Secret color Image and Cover images
  - 2: Output:  $S_1^{RGB}, S_2^{RGB}$  Shares
  - 3:  $SSCI^{RGB} \leftarrow$  Semantic image generation of  $SCI^{RGB}$
  - 4: For each channel  $SCI, CC^1, CC^2, CC^3$
  - 5: For each  $m$ : 1 to  $X$
  - 6: For each  $n$ : 1 to  $Y$
  - 7: do until( $m = X$  &  $n = Y$ )
  - 8:  $IS_{m,n}^1 \leftarrow \frac{SSCI}{100}$
  - 9:  $IS_{m,n}^2 \leftarrow rand([0,1], X, Y)$
  - 10:  $IS_{m,n}^3 \leftarrow \begin{cases} SI_{m,n} \bmod 10, & IS_{m,n}^2 = 1 \\ \frac{SI_{m,n}}{10} \bmod 10, & IS_{m,n}^2 = 0 \end{cases}$
  - 11:  $S_{m,n}^1 \leftarrow CC_{m,n}^1 - (CC_{m,n}^1 \% 10) + IS_{m,n}^1$
  - 12:  $S_{m,n}^2 \leftarrow CC_{m,n}^2 - (CC_{m,n}^2 \% 10) + IS_{m,n}^2$
  - 13:  $S_{m,n}^3 \leftarrow CC_{m,n}^3 - (CC_{m,n}^3 \% 10) + IS_{m,n}^3$
  - 14: End do
  - 15: End For
  - 16: End For
- 

In Algorithm 2, the methodology of the proposed SPEVSS is elaborated. Initially, the secret color image, represented as SCI, is converted into a semantic image labelled as SSCI. This SSCI is then encoded and broken down into intermediate shares: IS1, IS2, and IS3. Random coefficients are chosen for the pixel values of SSCI.

Subsequently, the shares, termed as IS1, IS2, and IS3, are formed by incorporating the intermediate shares IS1, IS2, and IS3 into cover images CC1, CC2, and CC3. This incorporation utilizes the Least Significant Bit (LSB) embedding method<sup>[14]</sup>. These crafted shares are then transmitted to authorized recipients via communication channels like third-party software, email platforms, and so on. The range for the intermediate shares is defined as  $IS1 \in \{0, 1, 2\}$ ,  $IS2 \in \{0, 1\}$ , and  $IS3 \in \{0, 1, 2, \dots, 9\}$ . The shares S1, S2, and S3 have a range of  $\{0, 1, 2, \dots, 255\}$ .

### 3.3. Pixel reconstruction stage

As depicted in **Figure 4**, a systematic process for this stage is provided. Initially, the received shares are categorized into three distinct color channels: Red (R), Green (G), and Blue (B). Each of these color channels undergoes a procedure known as LSB extraction. From this process, the Reconstructed Intermediate Shares, denoted as RIS1 and RIS2, are derived<sup>[14]</sup>. Subsequently, a unique key is generated from the obtained RIS values. An error threshold, represented by the number 9, is set. Utilizing this key, the Reconstructed Color Semantic Pixel (RSSCI) values are decoded from the retrieved RIS. RSSCI is then reconstructed by digitally stacking all the retrieved shares.



**Figure 4.** Reconstruction of secret color image.

---

#### Algorithm 3 Pixel Reconstruction Stage

---

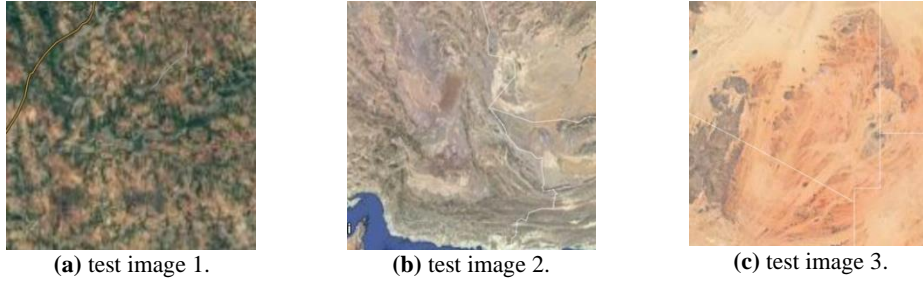
- 1: *Input:  $S^1, S^2, S^3$  Received Share Images*
  - 2: *Output: Reconstructed Secret Image RSSCI*
  - 3: *For each channel  $Sh^1, Sh^2, Sh^3$*
  - 4: *For each  $m$ : 1 to  $X$*
  - 5: *For each  $n$ : 1 to  $Y$*
  - 6: *do until  $(m = X \ \& \ n = Y)$*
  - 7:  $RIS_{m,n}^1 \leftarrow Sh_{m,n}^1 \% 10$
  - 8:  $RIS_{m,n}^2 \leftarrow S_{m,n}^2 \% 10$
  - 9:  $key_{m,n} \leftarrow TH - (RIS_{m,n}^1 + RIS_{m,n}^2)$
  - 10:  $RSI_{m,n} \leftarrow \begin{cases} RIS_{m,n}^1 \times 100 + RIS_{m,n}^3 \times 10 + key_{m,n}, & RIS_{m,n}^2 = 0 \\ RIS_{m,n}^1 \times 100 + key_{m,n} \times 10 + RIS_{m,n}^3, & RIS_{m,n}^2 = 1 \end{cases}$
  - 11: *End do*
  - 12: *End For*
  - 13: *End For*
- 

The algorithm outlined in the revealing phase employs straightforward calculations to decrypt the RSI. If any share is tampered with, falsified, or corrupted, the RSI is not unveiled.



## 4. Experimentation and result analysis

Experimental results for the proposed SPEVSS focus on three primary objectives: first, the generation of a high-quality reconstructed secret image; second, the achievement of reduced computational complexity; and finally, the assurance of no pixel expansion. The SPEVSS is adaptable and can be applied to secret color images of any size. The effectiveness of the method presented in this study was validated by implementing and executing the algorithm in the MATLAB 7.10 Tool. A comparative analysis was conducted between the quality of reconstructed images and the original secret images. For the purpose of testing, a selection of satellite images were considered, as displayed in **Figure 5a–c**.



**Figure 5.** Secret color test images.

**Figure 6a–c** presents a collection of cover images employed for the experimental analysis. These images, sourced from MATLAB's sample image set, serve as the external layer for the secret images<sup>[15,16]</sup>. It is essential that these cover images match the size of the secret images.



**Figure 6.** Color cover test images.



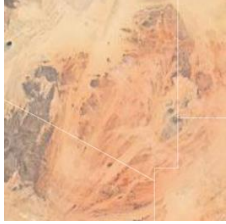


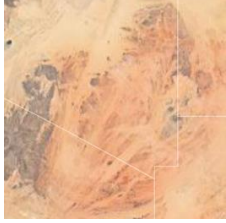
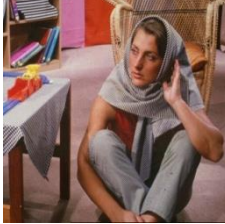
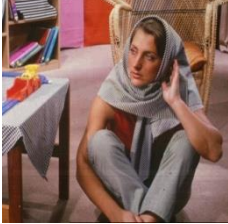
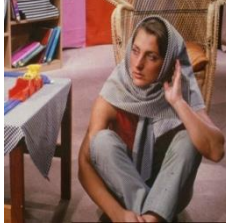
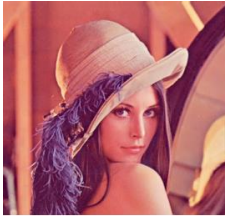
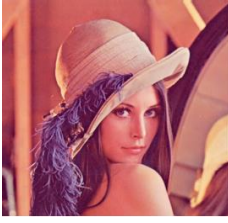
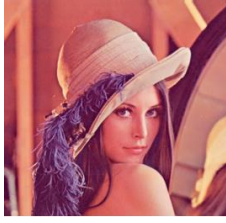






### 4.1. Quality analysis

Over 60 diverse test images, including Satellite images, natural scenes, and military map images, were utilized to evaluate the robustness and adaptability of the SPEVSS.

In the experiments conducted for the proposed SPEVSS, **Table 1** highlighted that individual shares concealed the secret information effectively, appearing as typical natural images, thus ensuring the share values are perceived as meaningful. The quality of the image is measured in terms of PSNR and ranges above 35 dB is considered to be accepted with good quality. If the quality of the secret and the reconstructed image is same then the optimal quality is achieved with PSNR as infinity  $\infty$ <sup>[17]</sup>. The quality assessment results are tabulated in **Table 2**.

As inferred from **Table 2**, the reconstructed image quality is impressive and within the acceptable range. The proposed SPEVSS does not increase the pixel size of the secret image. Hence, there will not be any pixel expansion.

**Table 1.** Life cycle of Proposed SPEVSS.

Secret image			
Pixel Encoding			
Share1			
Share2			
Share3			
Reconstructed Image			

**Table 2.** Quality values of Secret Image vs. Reconstructed image.

Test images	PSNR	MSE	SSIM	MAE
Test image 1	42.242	4.14873	0.936	2.56053
Test image 2	39.905	10.25	0.897	7.482
Test image 3	41.581	7.644	0.966	4.996
Test image 4	36.195	18.22	0.695	12.28



## 4.2. Security analysis

The efficiency of the proposed SPEVSS is gauged by its ability to securely transmit the secret image, contingent upon several conditions:

**Condition 1:** In the SPEVSS approach, a semantic encoding is employed to process the image semantically. Image pixels are then divided and randomly incorporated into cover images. As a result, the shares contain only minimal traces of the image, and these traces don't resemble the original image.

**Condition 2:** In the event of a malicious attack on the shares, they won't compromise the image. This is because any single share only contains fragments of encrypted pixel values, which are distributed randomly.

**Condition 3:** Shares appear as regular cover images, preserving their inherent quality, a testament to the efficacy of the proposed SPEVSS. The subsequent section delves deeper into image quality. By employing the LSB embedding technique, encrypted pixel values are seamlessly integrated with the cover images. This subtle integration diminishes the likelihood of an attacker suspecting the presence of a concealed message within the shares.

## 4.3. Comparative analysis

**Table 3** shows a comparative analysis of SPEVSS against existing methodologies, with evaluations based on certain criteria:

- Number of shares (Rule 1): Denotes the total share count produced using SPEVSS<sup>[17]</sup>.
- PSNR value of reconstructed secret image (Rule 2): Utilized to assess image similarities<sup>[12]</sup>.
- Shares generation technique (Rule 3): The method employed for share creation<sup>[18]</sup>.
- Shares size (Rule 4): The size of the secret color image  $I$  and the share sizes are compared.
- Computational complexity (Rule 5): Represents the time taken for executing the algorithm operations time complexity  $O(n)$ <sup>[19]</sup>.
- Pixel Expansion (Rule 6): Examines pixel size variations during the share construction phase<sup>[20]</sup>.

**Table 3.** Comparative analysis of SPEVSS with existing systems.

Scheme	[21]	[22]	[23]	[24]	Proposed SPEVSS
Rule 1	$n \geq 2$	$n = 2$	$n \geq 2$	$n \geq 2$	$n = 3$
Rule 2	22–27 dB	28–38 dB	23–28 dB	22–27 dB	33–43 dB
Rule 3	Pixel replacement	Ordered	Random	Pixel replacement	Random
Rule 4	$(2n + n + 1) \times N$	$N$	$N \times 1.05$	$(2n + 1) \times N$	$N$
Rule 5	High	Low	Medium	Very High	Very Low
Rule 6	$\geq 2$	None	$\geq 1$	$\geq 2$	None

**Table 3** accentuates the efficiency of SPEVSS in secure color image transmission. The SPEVSS exhibits superior PSNR values compared to other methods. In SPEVSS, the secret image  $I$  is transitioned into a semantic image  $SI$ , mitigating pixel errors during the share construction phase<sup>[8]</sup>. This transition ensures image quality preservation. SPEVSS introduces no pixel expansion during share generation<sup>[25,26]</sup> and minimizes computational complexity by adopting basic arithmetic operations during both share generation and secret image reconstruction. SPEVSS fortifies share image security by embedding them into cover images. Each share conceals the secret independently, ensuring unauthorized users with access to all shares remain clueless without the reconstruction algorithm. This analysis confirms that SPEVSS provides an efficient means to transmit secret color images with minimal computations while maintaining exceptional image quality.

## 5. Conclusion

This study explored a new method termed SPEVSS for securely transmitting images. An enhancement in the preservation of image quality while ensuring its security was observed with this method. When SPEVSS was compared to other existing methods, it outperformed in various aspects. Notably, the quality of images was better preserved, unnecessary enlargement of the image was avoided, and excessive computational power was not required. Further, it was confirmed that unauthorized access to the image rendered it incomprehensible. The original image could be accurately deciphered only when the correct procedures were employed. This research identified SPEVSS as an effective tool for secure image transmission. Its simplicity, quality preservation, and security measures were highlighted. Potential improvements and further research on this method can be pursued in future studies.

## Author contributions

Conceptualization, JBA and SMG; methodology, KP; software, JVB and MA; validation, SDB; investigation, CEKA and SRS; data curation, CEKA; writing—original draft preparation, JBA and SMG; writing—review and editing, KP. All authors have read and agreed to the published version of the manuscript.

## Conflict of interest

The authors declare no conflict of interest.

## References

1. Naor M, Shamir A. Visual cryptography. *Lecture Notes in Computer Science*. 1995, 1-12. doi: 10.1007/bfb0053419
2. Ito K, Takahashi Y. An Overview of Visual Cryptography Techniques. *Cryptographic Systems Journal*, 2020, 44(1), 12–25.
3. Arora A, Garg H, Shivani S. Privacy Protection of Digital Images Using Watermarking and QR Code-based Visual Cryptography. *Advances in Multimedia*. 2023, 2023: 1-9. doi: 10.1155/2023/6945340
4. Kang I, Arce GR, Lee HK. Color Extended Visual Cryptography Using Error Diffusion. *IEEE Transactions on Image Processing*. 2011, 20(1): 132-145. doi: 10.1109/tip.2010.2056376
5. Attaullah ST, Jamal SS. An Improved Chaotic Cryptosystem for Image Encryption and Digital Watermarking. *Wireless Personal Communications*. 2019, 110(3): 1429-1442. doi: 10.1007/s11277-019-06793-1
6. Yang CN, Sun LZ, Cai SR. Extended color visual cryptography for black and white secret image. *Theoretical Computer Science*. 2016, 609: 143-161. doi: 10.1016/j.tcs.2015.09.016
7. Aswad FM, Salman I, Mostafa SA. An optimization of color halftone visual cryptography scheme based on Bat algorithm. *Journal of Intelligent Systems*. 2021, 30(1): 816-835. doi: 10.1515/jisys-2021-0042
8. Selva Mary G, Manoj Kumar S. A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication. *Measurement Science and Technology*. 2019, 30(12): 125404. doi: 10.1088/1361-6501/ab2faa
9. Ibrahim D, Sihwail R, Arrifin KAZ, et al. A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm. *Symmetry*. 2023, 15(7): 1305. doi: 10.3390/sym15071305
10. Çiftci E, Sümer E. A novel steganography method for binary and color halftone images. *PeerJ Computer Science*. 2022, 8: e1062. doi: 10.7717/peerj-cs.1062
11. Selva Mary G, Blesswin AJ, Kumar SM. Self-authentication Model to Prevent Cheating Issues in Grayscale Visual Secret Sharing Schemes. *Wireless Personal Communications*. 2022, 125(2): 1695-1714. doi: 10.1007/s11277-022-09628-8
12. Rani N, Sharma SR, Mishra V. Grayscale and colored image encryption model using a novel fused magic cube. *Nonlinear Dynamics*. 2022, 108(2): 1773-1796. doi: 10.1007/s11071-022-07276-y
13. Selva Mary G, Manoj Kumar S. Secure grayscale image communication using significant visual cryptography scheme in real time applications. *Multimedia Tools and Applications*. 2019, 79(15-16): 10363-10382. doi: 10.1007/s11042-019-7202-7
14. Somwanshi DR, Humbe VT. A Secure and Verifiable Color Visual Cryptography Scheme with LSB Based Image Steganography. *International Journal of Advanced Trends in Computer Science and Engineering*, 2021, 10(4), 2669–2677.
15. Wang L, Yan B, Yang HM, et al. Flip Extended Visual Cryptography for Gray-Scale and Color Cover Images. *Symmetry*. 2020, 13(1): 65. doi: 10.3390/sym13010065

16. Wu X, Yang CN. Probabilistic color visual cryptography schemes for black and white secret images. *Journal of Visual Communication and Image Representation*. 2020, 70: 102793. doi: 10.1016/j.jvcir.2020.102793
17. Blesswin J, Mary S, Suryawanshi S, et al. Secure transmission of grayscale images with triggered error visual sharing. *Journal of Autonomous Intelligence*. 2023, 6(2): 957. doi: 10.32629/jai.v6i2.957
18. Qi Wang, John Blesswin A, et al. Securing image-based document transmission in logistics and supply chain management through cheating-resistant visual cryptographic protocols. *Mathematical Biosciences and Engineering*, 2023, 20(11): 19983-20001. doi: 10.3934/mbe.2023885
19. Pan JS, Liu T, Yang HM, et al. Visual cryptography scheme for secret color images with color QR codes. *Journal of Visual Communication and Image Representation*. 2022, 82: 103405. doi: 10.1016/j.jvcir.2021.103405
20. Salim MZ, Abboud AJ, Yildirim R. A Visual Cryptography-Based Watermarking Approach for the Detection and Localization of Image Forgery. *Electronics*. 2022, 11(1): 136. doi: 10.3390/electronics11010136
21. Blesswin J, Mary S, Gobinath T, et al. Error-induced inverse pixel visual cryptography for secure QR code communication. *Journal of Autonomous Intelligence*. 2023, 7(1). doi: 10.32629/jai.v7i1.1129
22. Zhang D, Ren L, Shafiq M, et al. A Privacy Protection Framework for Medical Image Security without Key Dependency Based on Visual Cryptography and Trusted Computing. *Computational Intelligence and Neuroscience*. 2023, 2023: 1-11. doi: 10.1155/2023/6758406
23. Hodeish ME, Humbe VT. An Optimized Halftone Visual Cryptography Scheme Using Error Diffusion. *Multimedia Tools and Applications*. 2018, 77(19): 24937-24953. doi: 10.1007/s11042-018-5724-z
24. John Blesswin A, Selva Mary G, Manoj Kumar S. Multiple Secret Image Communication Using Visual Cryptography. *Wireless Personal Communications*. 2021, 122(4): 3085-3103. doi: 10.1007/s11277-021-09041-7
25. John Blesswin A, Mary S, Gobinath T, et al. Error-induced inverse pixel visual cryptography for secure QR code communication, *Journal of Autonomous Intelligence*. 2023, 7(1): 1129.
26. Sherine A, Peter G, Stonier AA, et al. CMY Color Spaced-Based Visual Cryptography Scheme for Secret Sharing of Data. *Wireless Communications and Mobile Computing*. 2022, 1–12.