Mathematical Biosciences and Engineering

MBE, 20(11): 19983–20001.
DOI: 10.3934/mbe.2023885
Received: 02 September 2023
Revised: 14 October 2023
Accepted: 24 October 2023
Published: 02 November 2023

http://www.aimspress.com/journal/MBE

Research article

Securing image-based document transmission in logistics and supply chain management through cheating-resistant visual cryptographic protocols

Qi Wang[1], John Blesswin A[2,*], Manoranjitham T[3], Akilandeswari P[3], Selva Mary G[2,*], Shubhangi Suryawanshi[4] and Catherine Esther Karunya A[5]

[1] Teacher's College of Beijing Union University, Beijing Union University, Beijing, China
[2] Directorate of Learning and Development, SRM Institute of Science and Technology, Kattankulathur 603203, India
[3] Department of Computing Technologies, School of Computing, SRM Institute of Science and Technology, Kattankulathur 603203, India
[4] Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Pimpri 411018, India
[5] Department of Artificial Intelligence and Machine Learning, SNS College of Technology, Coimbatore 641035, India

* **Correspondence:** Email: selvamaryg.rnd@gmail.com, johnblesswin.rnd@gmail.com.

Abstract: In today's digital landscape, securing multimedia visual information—specifically color images—is of critical importance across a range of sectors, including the burgeoning fields of logistics and supply chain management. Traditional Visual Cryptography (VC) schemes lay the groundwork for encrypting visual data by fragmenting a secret image into multiple shares, thereby ensuring no single share divulges the secret. Nevertheless, VC faces challenges in ascertaining the integrity of reconstructed images, especially when shares are manipulated maliciously. Existing solutions often necessitate additional shares or a trusted third party for integrity verification, thereby adding complexity and potential security risks. This paper introduces a novel Cheating-Resistant Visual Cryptographic Protocol (CRVC) for Color Images that aims to address these limitations. Utilizing self-computational models, this enhanced protocol simplifies the integrated integrity verification process, eliminating the need for extra shares. A standout feature is its capability to securely transmit meaningful shares for color images without compromising the quality of the reconstructed image as the PSNR maintains to be ∞. Experimental findings substantiate the protocol's resilience against

quality degradation and its effectiveness in verifying the authenticity of the reconstructed image. This innovative approach holds promise for a wide array of applications, notably in sectors requiring secure document transmission, such as Logistics and Supply Chain Management, E-Governance, Medical and Military Applications.

Keywords: visual cryptography; cheating-resistant; integrity verification; color image encryption; logistics communication; security; self-authentication

1. Introduction

Logistics and supply chain management have long been the backbone of global commerce. The advent of new technologies such as Big Data analytics, IoT, and Industry 4.0 have revolutionized this domain, offering unprecedented levels of efficiency and analytical insights. However, these advancements are not without their challenges. One often-overlooked aspect is the security of image-based digital documents, which are increasingly being communicated through social media platforms like WhatsApp and Telegram for convenience. Given the sensitive nature of these documents, which could range from invoices to shipping manifests, their secure transmission becomes a critical concern [1]. Visual Cryptography (VC). Introduced by Naor and Shamir in 1994, VC offered a unique approach to encrypting visual information. Instead of traditional cryptographic methods that transform an image into an incomprehensible series of numbers and letters, VC divides an image into multiple shares or pieces. When these shares are stacked or overlaid, they reconstruct the original image. However, these shares provide no discernible information about the original, ensuring the secret remains safe even if some shares are exposed [2]. Initially, VC was designed to handle binary images, which are black-and-white images with each pixel entirely black or white. However, as technology and research advanced, VC extended its capabilities to handle grayscale images and, more recently, colour images [3]. While this evolution has expanded the scope of VC, it has also introduced complexities. Despite its promise, VC has its challenges. One of the primary issues VC faces is verifying the integrity of the reconstructed image [4]. Since the secret is divided among several shares, altering even a single share can affect the final reconstructed image's integrity [5]. Traditional methods of checking this integrity involve additional shares or a trusted third party, complicating the process and introducing potential security vulnerabilities [6]. In light of these challenges, exploring advanced VC protocols specially tailored for colour images in sectors like E-Governance is imperative. These protocols should ensure secure encryption and provide mechanisms to ascertain the integrity and authenticity of the reconstructed image without added complexities. Table 1 provides definitions and explanations for key terms that are important for understanding the research presented in this article.

Ensuring the integrity and authenticity of reconstructed images in such a domain is both a golden opportunity and a stringent requirement. To bridge the existing gaps and address the inherent challenges, this research delineates four pivotal objectives such as; Engineer a cheat-resistant Visual Cryptography algorithm tailored for color images, aiming to mitigate the risks associated with share tampering; Embed an integrity verification mechanism within the algorithm, to autonomously ensure the authenticity of the reconstructed images without relying on external entities or additional shares; Strive to uphold the quality of the reconstructed color images, ensuring that the visual clarity and

information integrity are not compromised; Conduct a comparative analysis, juxtaposing the proposed algorithm against existing methodologies to highlight the advancements and the added value brought forth by this research. Through the meticulous pursuit of these objectives, this research aims to contribute a robust solution to the existing discourse, fostering enhanced security and authenticity in Visual Cryptography, especially within the critical domain of E-Governance.

Table 1. Glossary of key terms and concepts in CRVC.

Notation	Explanation
CSC	Color secret content: The original color image that contains confidential or sensitive information.
$\mathrm{CSC}^R, \mathrm{CSC}^G \ and \ \mathrm{CSC}^B$	Color channels of color secret content.
MK	Master key: A set of random numbers used for the initial encryption of the color secret content.
MKS	Master segmented key: A portion of the master key used in various stages of the encryption process.
COI	Cover overlay image: A natural or specific color image used to disguise the color secret content.
MS	Meaningful Share: The ciphered portion of the color secret content, encrypted using the master and segmented keys.
$TE \ \ RD$	Transmission encoding and receiving decoding: The process of encoding the color secret content for secure sending and decoding it upon receiving.
TDP	Transitional decoded pixels: Temporary decoded pixel values generated during the decryption process at the receiver's end.
REV	Received Encrypted Values: The pixel values of the shares received at the receiver end
$RMSK$	Received Master Segmented Key: A portion of the master key generated during decryption process.
IS	Intermediate Secret: Part of the color image pixels reconstructed at the receiver end
VP	Verification Pixels: Pixels generated during decryption process for self-authenticating
VS	Verification Status: Binary value generated during verification process.
$RCSC$	Reconstructed color Secret content: The decrypted color image that is revealed at the receiver's end.
VP	Verification pixels: Specific pixel values generated to confirm the integrity of the unveiled color content.
VS	Verification status: A binary value (1 or 0) that indicates whether the integrity verification of the unveiled color content was successful or not.

The rest of the research paper is organized as Section 2 delves into an extensive literature study, offering insights into the historical development and current state-of-the-art visual cryptography,

focusing on integrity verification and applications in E-Governance. Section 3 introduces the Proposed Cheating-Resistant Visual Cryptographic Protocol, detailing the algorithmic design and the built-in integrity verification mechanisms specific to color images. Section 4 presents the Experimentation and Result Analysis, where the performance metrics of the proposed protocol are rigorously evaluated through a series of tests. Section 5 provides a Comparative Analysis wherein the proposed scheme is benchmarked against existing security, integrity assurance, and computational efficiency methods. Finally, Section 6 summarizes the paper, concluding the essential findings and suggesting avenues for future research.

2. Review of literature

The science of Visual Cryptography (VC) has garnered significant attention since its inception. Naor and Shamir pioneered the concept of visual cryptography, where an image was divided into shares [1]. This division ensured that a combination of these shares would reveal the original image, but individually, they were indistinguishable. This foundational work set the stage for numerous advancements in the field. Ateniese et al. delved deeper into the concept, bringing forth extended capabilities for visual cryptography [7]. Their work addressed the limitations of the original model, providing a broader scope for VC's application. As the digital world progressed, the need for more advanced encryption techniques for diverse data types became evident. Elashry et al. proposed a novel method for encrypting images with minimal details using the Rijndael and RC6 block cyphers, emphasizing the importance of robust encryption techniques in a digitally pervasive environment [8]. The dynamic nature of visual cryptography and its adaptability to various scenarios were explored by Sian and Wei [9]. Their probabilistic model demonstrated VC's potential in flexible and ever-changing environments, emphasizing its relevance in today's volatile digital landscape. The application of VC was not just limited to binary images. Lin and Tsai expanded the horizons by introducing visual cryptography for grey-level images using dithering techniques, further enhancing VC's versatility [10]. The realm of grayscale images in visual cryptography was challenging. A meticulous approach to improving the visual quality of grayscale images in VC was presented by Blesswin et al. [11–13]. Their study shed light on the intricacies of ensuring the reconstructed image retains its visual fidelity, even as the encryption mechanism becomes more sophisticated. In the same vein, the study by Wang and Arce presented a novel approach that amalgamated halftone visual cryptography with error diffusion [14]. Mary et al. delved deep into this realm, emphasizing the importance of optimal grayscale visual cryptography for secure image communication in governance structures [15,16]. Their work underscores the broader societal implications of robust VC techniques. Furthermore, the extensive study by Pan et al. brought forth an efficient QR-code authentication protocol leveraging visual cryptography [17]. In an era where QR codes have become ubiquitous, especially in sectors like E-Governance. Cheng et al. took the conversation on QR codes further [18]. Their study, which proposed a VC scheme for QR codes that produced meaningful shares, emphasized the user-centric aspect of VC. In real-world applications, having meaningful shares, rather than random patterns, can enhance user trust and confidence in the system. The literature also reflects an increasing focus on the collaborative aspects of VC. Guo et al. presented collaborative visual cryptographic schemes that pave the way for multi-party secure visual data sharing [19]. Their work is a testament to VC's adaptability to collaborative and distributed environments. One of the recurring themes in the literature is the challenge of cheating prevention in VC. Ren et al. tackled this head-on with their visual cryptography

scheme using Latin square, aiming to make the VC process more resistant to malicious actors and ensure the reconstructed image's integrity [20]. With the digitization of governance, the need for secure transmission and storage of visual information became paramount. Several studies have highlighted the potential of VC in E-Governance [6]. The ability of malicious attackers to tamper with the shares in Visual Cryptography underscores the importance of developing cheat-resistant algorithms and incorporating built-in integrity verification mechanisms. Such advancements are crucial in safeguarding the reconstructed images against potential tampering and ensuring the authenticity and reliability of the visual information, especially in sensitive applications like E-Governance. The exploration of mobile malicious attackers in the mentioned study enriches the broader narrative on system security, providing valuable insights and methodologies that could be leveraged in addressing the challenges inherent in Visual Cryptography. By adopting a holistic approach, encompassing the lessons learned from general random system security, this research aims to develop a more robust and reliable Visual Cryptography framework capable of withstanding malicious activities and ensuring the integrity of reconstructed images [7,8].

Despite its potential, VC has its set of challenges. The integrity verification of reconstructed images has been a recurring theme in the literature. As the secret is distributed among various shares, ensuring the integrity of the final image, especially when a share might be tampered with, is crucial. Some solutions involved additional shares or a third-party verifier, but these often added complexity and potential vulnerabilities [21]. The literature reveals a consistent interest in Visual Cryptography and its applications over the years. Challenges remain while significant advancements have been made, especially in extending VC to colour images and meaningful shares. The domain of E-Governance, with its specific needs and sensitivities, presents both an opportunity and a demand for further research, especially in ensuring the integrity and authenticity of reconstructed images. To address these gaps and challenges, this research aims to focus on four key objectives:

- Develop a cheat-resistant Visual Cryptography algorithm for color images.
- Incorporate built-in integrity verification.
- Maintain the quality of the reconstructed color image.
- Compare the proposed algorithm with existing methods.

Through these objectives, this research aims to advance VC, particularly in applications requiring high levels of security and integrity, such as E-Governance.

3. Proposed cheating-resistant visual cryptographic protocol

The secure transmission of visual data, particularly color images, is an increasing concern and scrutiny area. While colour images serve as a crucial medium for conveying complex and nuanced information across various sectors, the susceptibility of these images to unauthorized access and tampering presents a significant security risk. A novel framework—CRVC, is proposed to fulfil multiple objectives critical to secure visual data transmission: (i) To offer a high level of security, ensuring that the color image data remains confidential during transmission. (ii) To maintain the colour image’s quality, ensure that the reconstructed image retains its original clarity and resolution. (iii) To incorporate an integrity verification phase, allowing the receiver or a separate authenticator to confirm that the reconstructed color image has not been tampered with during transmission [22,23].

The CRVC methodology comprises three critical phases, each serving a specific function: sender-side encoding, receiver-side decoding and verifier-side authentication process.

The protocol is designed to resist cheating, ensuring that even if some of the shares are altered, the integrity verification step will identify any discrepancies. This multi-faceted approach makes CRVC a comprehensive solution for secure colour image transmission, with potential applications in diverse sectors, including E-Governance, healthcare, and defence. The detailed methodology of the proposed CRVC is shown in Figure 1.

Figure 1 shows the overall architecture of the proposed CRVC. This proposed CRVC aims to transmit a single Color image (CSC) from the sender to the receiver in a secure manner.

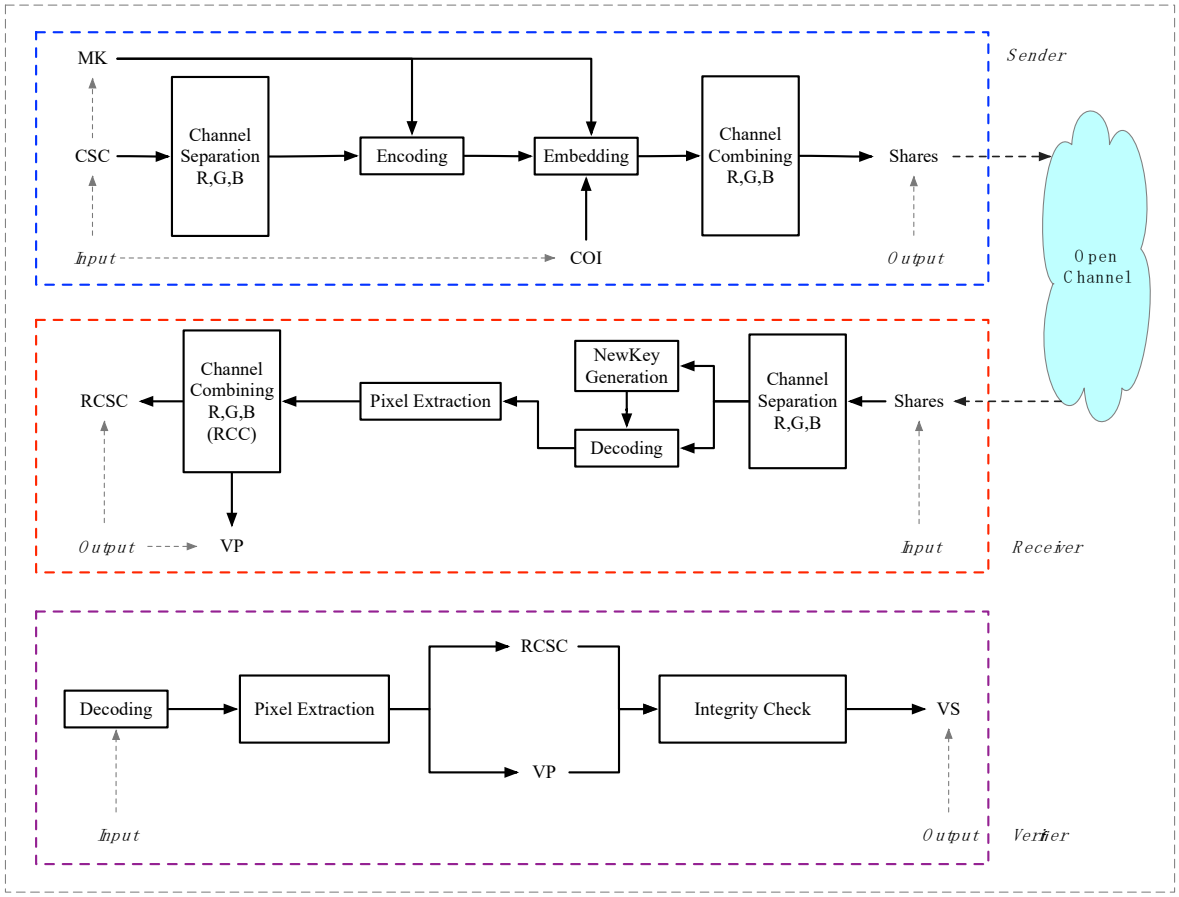


Figure 1. Architecture of proposed CRVC.

3.1. Sender-side encoding phase

An asymmetric key is used in this proposed CRVC. A Master Key (MK) is used to encode the image for increased security. The steps involved in this phase is as follows:

Step 1: In the Sender-side Encoding Phase, a color secret image CSC is divided into its Red, Green and Blue (RGB) channels: $\mathrm{CSC}^R, \mathrm{CSC}^G$ *and* CSC^B.

Step 2: Master Key*(MK)* Matrix Generation: MK matrix is generated, the dimensions of which match each RGB channel of CSC. The matrix values are randomly selected from a set of predetermined prime numbers. Equation (1) defines how MK is generated:

$$MK = \{xi \cup (xi \times yi)\}, where \;\; xi, yi \in \{7,11,13\} \tag{1}$$

Step 3: Master Segmented Key (MSK): The MK is divided into MSK, which are distributed along with the encrypted message and MK to the participants. MSK is constructed using Eqs (2)–(4):

$$MSK_1 = \begin{cases} 0, & \forall\ MK_i \leq m \\ 1, & otherwise \end{cases} \tag{2}$$

$$MSK_2 = \begin{cases} MK_i\ mod\ 10, & \forall\ MK_i \leq m \\ MK_i\ /\ 10, & otherwise \end{cases} \tag{3}$$

$$MSK_3 = \begin{cases} MK_i/\ 10, & \forall\ MK_i \leq m \\ MK_i\ mod\ 10, & otherwise \end{cases} \tag{4}$$

Here, m is a random median value of MK.

Step 4: Encoding Using Karatsuba Fast Multiplication (KFM): Each RGB channel and MK are encoded using the KFM method to generate intermediate Encrypted Values (EV) for each pixel in CSC using Eq (5):

$$EV = KFM(CSC, MK) \tag{5}$$

Step 5: Least Significant Bit (LSB) Embedding: The intermediate encrypted values EV are then embedded into Cover Overlay Images (COI) using the Least Significant Bit (LSB) embedding process. COI is a set of natural color images used to cover the secret values $EI\ and\ MSK$. The covered images are termed Meaningful Shares (MS) and are distributed to the participants. MS is constructed using Eq (6) [24–26]:

$$MS = LSB(COI, (EV, MSK)) \tag{6}$$

Here, MS appears like any natural color images of individual channels of Red, Green and Blue. Individual MS does not reveal any information about CSC.

Step 6: Channel Recombination: Reassemble the RGB channels from the received color shares MS using Eq (7).

$$MS = RGB(MS^R, MS^G\ and\ MS^B) \tag{7}$$

where MS is the set of shares where $|MS| = 6n$ where n is the number of secret image.

3.2. Receiver-side decoding phase

In the revealing phase, a group of authenticated participants digitally superimposes the received meaningful shares to reconstruct the original color content. The steps for the revealing phase are as follows:

Step 1: Collect the shares from the participants and separate the color channels and for each channel continue Steps 2 to 5.

Step 2: LSB extraction Process; The Received Meaningful Shares (RMS) received from the participants are digitally stacked. Using the Least Significant Bit (LSB) extraction process, the shares are separated into Received Encrypted Values (REV) and Received Master Segmented Key($RMSK$) using Eq (8):

$$\{REV_x, RMSK_y\} = LSB(RMS) \text{ where } x \leq t, y \leq k,\ t < n \ and \ t + k = n \tag{8}$$

Here, n represents the total number of shares distributed to the participants.

Step 3: Decoding: The subsets of the encrypted $RMSK_1$, $RMSK_2, RMSK_3$ are digitally stacked together, and a new Revealing Master Key($RMKey$)is generated using Eq (9):

$$RMKey = \begin{cases} \frac{T_{max}}{RMSK_2 \times 10 + \ RMSK_3}, \ \forall \ RMSK_1 = 0 \\ \frac{T_{max}}{RMSK_3 \times 10 + \ RMSK_2}, \ otherwise \end{cases} \tag{9}$$

In this equation, T_{max} is a constant multiple of the key values chosen during share generation. *Step 4:* Pixel Extraction: The Karatsuba Fast Multiplication (KFM) method is used for all multiplications involved in decrypting the secret. The REV values are digitally stacked together, and using $RMKey$, the Intermediate Secret (IS) color image is reconstructed using Eq (10):

$$IS = \ KFM(REV, RMKey) \tag{10}$$

Finally, the original color content Reconstructed Color Secret Content ($RCSC$) is obtained from IS using Eq (11):

$$RCSC = IS \ mod \ 10^{\frac{n}{2}} \tag{11}$$

Here, n is the length of the retrieved IS.

Step 5: Channel Recombination: Reassemble the RGB channels from the $RCSC$ using Eq (12).

$$RCSC = RGB(RCSC^R, RCSC^G \ and \ RCSC^B) \tag{12}$$

In this section the received shares were decoded and the RCSC is reconstructed using the RMSK.

3.3. Verifier-side authentication phase

Methods In the CRVC, the integrity of the reconstructed color content is of utmost importance. Integrity, in this context, refers to ensuring that the $RCSC$ has not been tampered with or altered. This verification is not meant to protect data from unauthorized access but to ensure its consistency and accuracy. The verifier phase is shown in Figure 2.

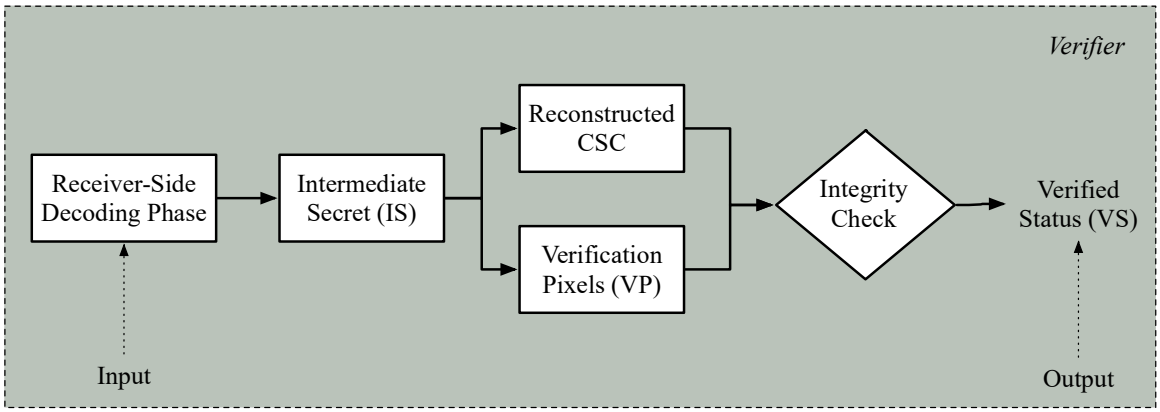


Figure 2. Working of Verifier-side Authentication Phase.

During the receiver side decoding phase, the IS pixel values are extracted and receiver-end two images namely, RCSC and VP are obtained using Eq (11) in the decoding phase and Eq (13).

$$VP = \frac{IS}{10^{\frac{n_{max}}{2}}} \tag{13}$$

n_{max} is calculated as the maximum length of the IS retrieved using Eqs (14) and (15).

$$n_{max} = floor(\log_{10}|IS_{(\max)}|) + 1 \tag{14}$$

$$IS_{(\max)} = \max_{1 \le i,j \le i*j} CSC \tag{15}$$

After establishing the Verification Pixels (VP), a Verification Status (VS) is computed for each pixel in the $RCSC$ using Eq (16):

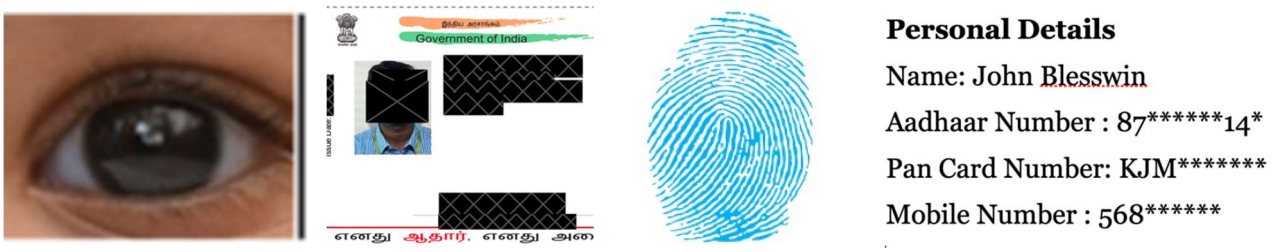
$$VS = \begin{cases} 1, & RCSC = VP \\ 0, & otherwise \end{cases} \tag{16}$$

If $VS = 1$ for all pixels, this indicates that the $RCSC$ is reliable, and its integrity has been verified. On the other hand, if $VS = 0$ for any pixel, it suggests that the RCSC may be compromised and should be considered unreliable. In the proposed CRVC, the original Color Secret Content (CSC) is divided into color channels. Each channel is encrypted separately using the Master Key (MK). This MK is then segmented into multiple Master Segmented Keys (MSKs).

Both the segmented MSKs and the CSC channels are encoded using the MK. The encoded values are then concealed within a Cover Overlay Image (COI) using the Least Significant Bit (LSB) embedding process. These disguised shares, called Encrypted Images (EIs), are distributed to the designated recipients. Upon receiving the shares, participants decode them to obtain the Reconstructed Color Content (RCC) and Verification Pixels (VP). At the verification stage, the RCC is compared with the VP to validate the image's integrity, thereby confirming or disproving its authenticity. In the next section, the experimentation and the result analysis of the proposed CRVC is explained.

4. Experimentation and result analysis

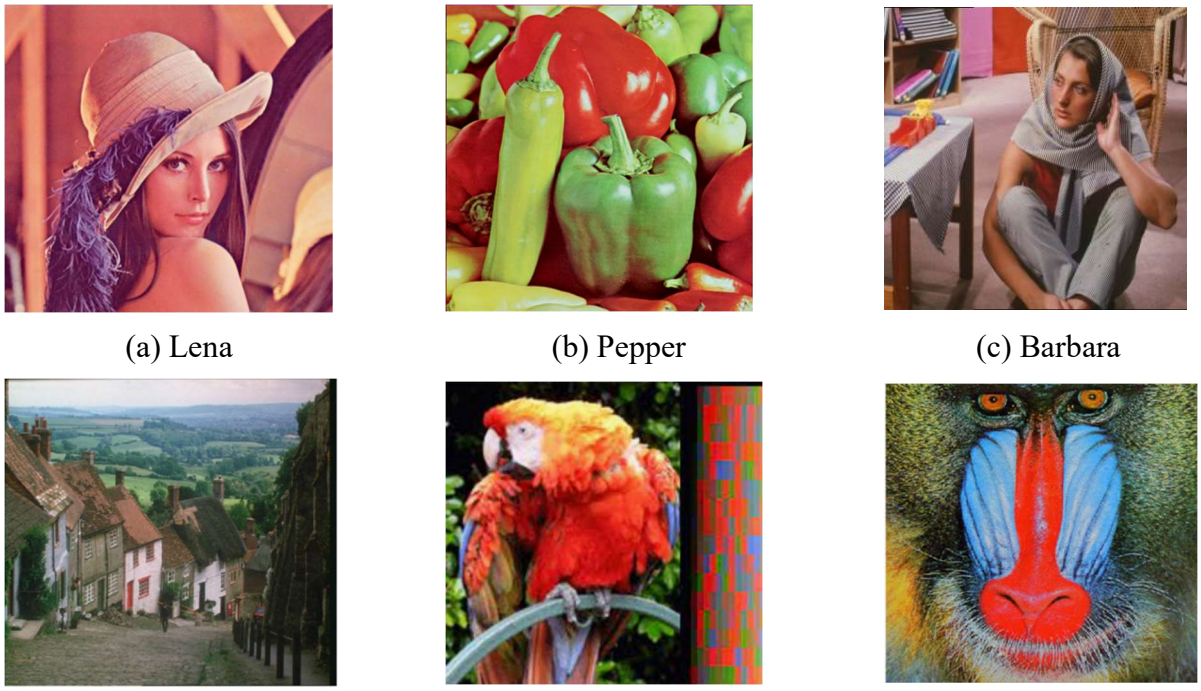
The primary focus of the CRVC is to ensure the security of the CSC, enhance the quality of the Reconstructed Color Content (RCC), and validate the integrity of the image with minimal computational overhead. The CRVC has been implemented using MATLAB, and the results are rigorously analysed [27]. Over 70 diverse sample test images spanning different sizes and color depths were employed for the tests. The efficiency of CRVC is compared with traditional visual cryptographic methods such as Verifiable Secret Image Sharing (VSIS), self-verifiable computational visual cryptographic protocol (SCVCP), Cheating prevention by self-authentication (CPS) and self-verifying visual secret sharing scheme (SVVSS). Figure 3 displays the variety of sample test images used for experimentation. These include Personal Identification Information (PII), biometric data and other images containing sensitive information. These images are assumed to be potentially sensitive and are used solely for experimental purposes.



(a) Eye Biometric (b)Aadhaar PII (c) Thumb (d) Sensitive details

Figure 3. Sample CSC for the study.

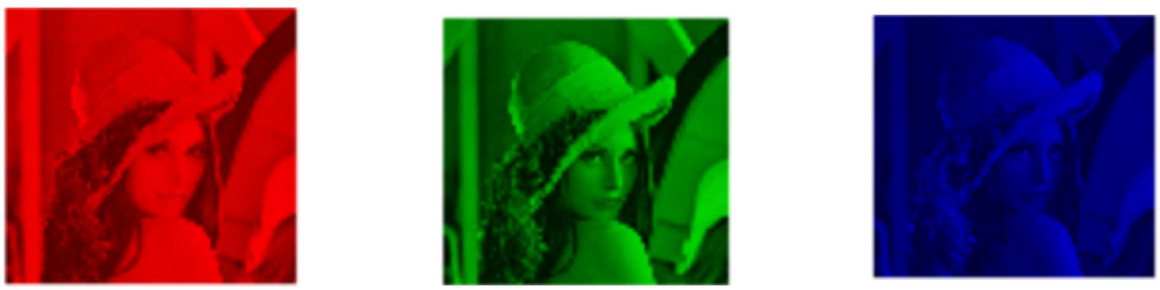
Figure 4 showcases the sample images used as COI. These images are publicly accessible and serve as the disguise for the encrypted color channels.



(a) Lena (b) Pepper (c) Barbara

(d) Goldhill (e) Bird (f) Baboon

Figure 4. Sample COI for the study.



(a) Red Channel (b) Blue channel (c) Green channel

Figure 5. Sample individual color channel of COI Lena Image.

Figure 5 shows the Red, Green and Blue channels of the COI Lena image for representation of individual channels where the pixel values of each channel varies from 0 to 255.

4.1. Results and life cycle of the proposed CRVC

The results of the share generation phase are illustrated in Figure 6. In this phase, a Thumb image is taken as an example for the CSC. The Master Key (MK) is randomly generated from a set of predefined integers. This MK is then segmented into MSKs. Both the CSC and the MK are encoded to generate intermediate encrypted shares (EV) using the Key-based Encoding Technique. These intermediate shares are then embedded into the COI using the Least Significant Bit (LSB) method, resulting in meaningful shares that are then distributed to authenticated participants [28].

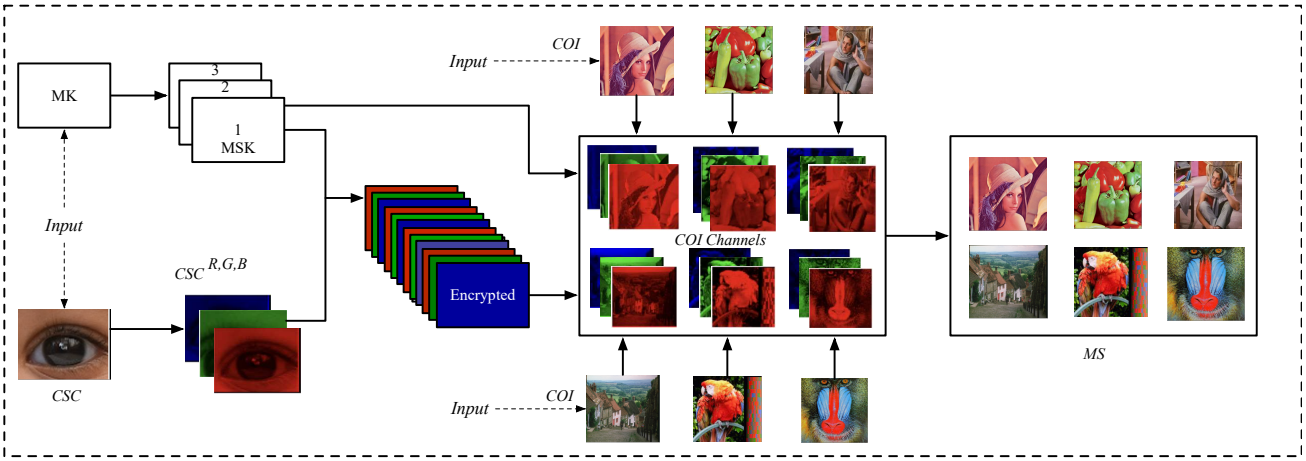


Figure 6. Sender side lifecycle of the CSC eye biometric.

Figure 7 depicts the revealing phase. During this stage, the Transmission Encoding and Receiving Decoding (TE and RD) process separates the encrypted shares into their corresponding color channels and MSKs using the LSB extraction method.

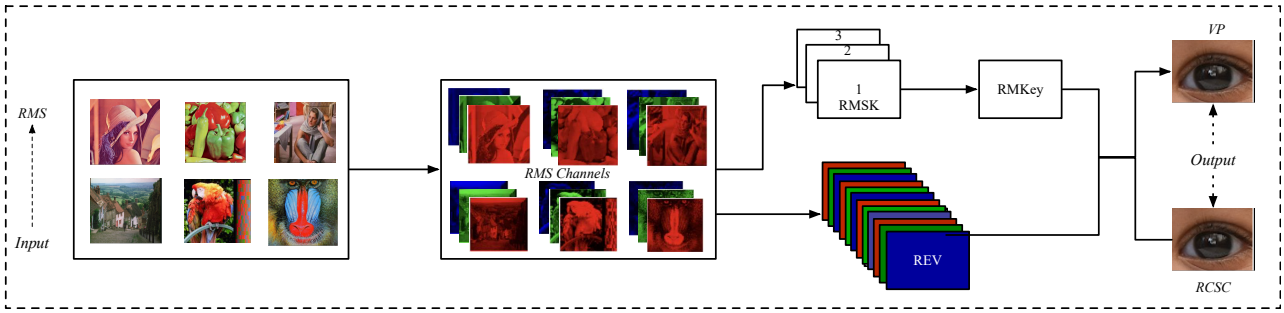


Figure 7. Receiver side lifecycle of the CSC eye biometric.

A new Received Master Key (RMK) is generated from the authenticated group of Received RMSKs, different from the original MK used for encryption. The color channels are then stacked together to form the TDP. These TDPs are further decoded to reveal the original Reconstructed Color

Secret Content (RCSC).

Figure 8 shows the verifier end of the proposed CRVC. In this phase the REV and RMSK's generated from the receiver end are considered and a new RMKey is generated. values, then the CSC is compromised.

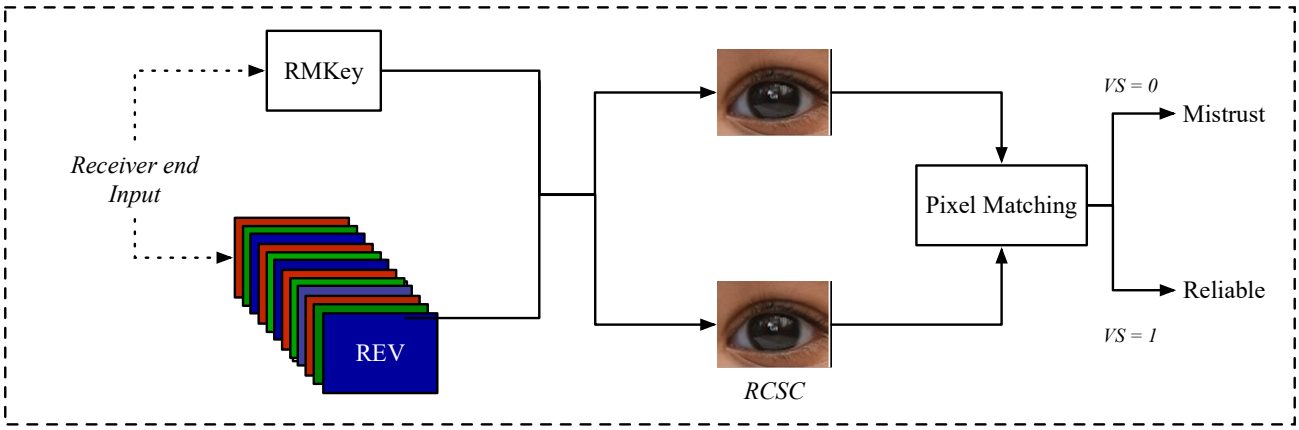


Figure 8. Verifier side lifecycle of the CSC eye biometric.

Using the RMK and the REV the encrypted pixels are decoded and provides the RCSC and the VP. Verifier takes the VP and the RCSC to compare the pixel values. This provides the VS to the verifier. Id the VS is 1 it implies the integrity of the secret is maintained and the if the VS is 0 for any of the pixel.

4.2. Results analysis

The primary objective of the CRVC is to enhance the security features of the CSC. While many cryptographic protocols emphasize confidentiality, CRVC places a special focus on integrity verification, along with other key security attributes like authentication.

4.2.1. Integrity verification

Integrity in CRVC is maintained through a meticulous encryption algorithm employed during the share generation phase. The Master Key (MK) is encrypted, then segmented into MSKs, which are subsequently distributed among multiple participants. This layered security approach is designed to ensure that the CSC remains unaltered and intact throughout the process, from encryption to decryption. The shares themselves appear as natural images, providing no clues to an intruder about the number of shares or their content. If an intruder were to collect all the shares, they would still need to go through the revealing phase to reconstruct the CSC, and even then, they would be subjected to integrity checks. Table 2 illustrates the efficacy of CRVC's integrity verification measures under various scenarios.

Table 2. CRVC Performance with integrity verification.

CSC	MS1	MS2	MS3	MS4	MS5	MS6	VS	Result
Test 1	Reliable	Reliable	Reliable	Reliable	Reliable	Reliable	1	Authentic
Test 2	Fake	Reliable	Reliable	Reliable	Reliable	Reliable	0	Forged
Test 3	Reliable	Fake	Reliable	Reliable	Reliable	Reliable	0	Forged
Test 4	Reliable	Reliable	Fake	Reliable	Reliable	Reliable	0	Forged
Test 5	Reliable	Reliable	Reliable	Fake	Reliable	Reliable	0	Forged
Test 6	Reliable	Reliable	Reliable	Reliable	Fake	Reliable	0	Forged
Test 7	Reliable	Reliable	Reliable	Reliable	Reliable	Fake	0	Forged
Test 8	Reliable	Fake	Reliable	Fake	Reliable	Reliable	0	Forged
Test 9	Reliable	Reliable	Fake	Fake	Fake	Reliable	0	Forged
Test 10	Reliable	Reliable	Reliable	Fake	Fake	Fake	0	Forged

The results indicate that the protocol effectively detects any unauthorized or tampered shares, thereby confirming its robustness in maintaining the integrity of the CSC. This makes CRVC particularly suitable for applications where the integrity of sensitive color images is a critical requirement.

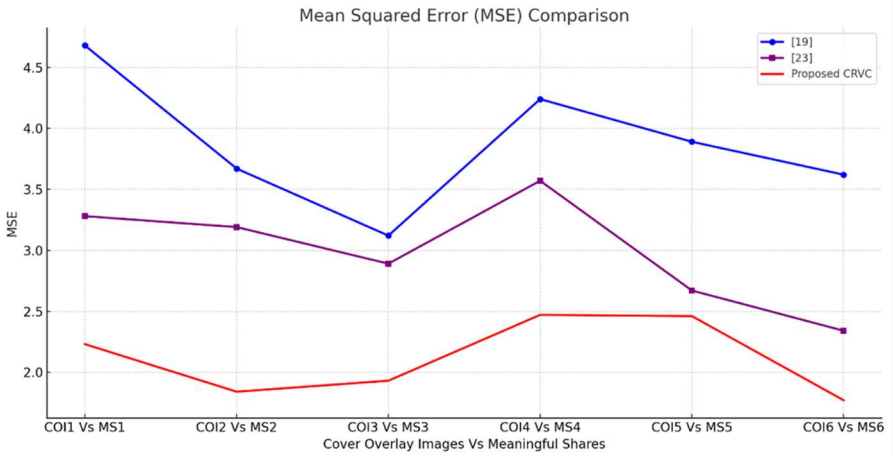
4.2.2. Quality analysis

To analyse the quality of the Reconstructed Color Secret Content (RCSC), metrics like Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index (SSIM) are employed. A lower MSE corresponds to a higher PSNR, indicating better image quality. If MSE approaches zero, the images are highly similar. Images with a PSNR above 25 dB are considered good quality, and higher values signify a better resemblance to the original. SSIM serves as a measure of structural similarity between two images, ranging from −1 to +1. A value of +1 indicates that the images are identical in structure [29,30]. Figure 9 presents the quality metrics where individual shares are compared with the original COI, PSNR, MSE, and SSIM values are calculated to assess the efficacy of CRVC in maintaining the integrity and quality of the shares.

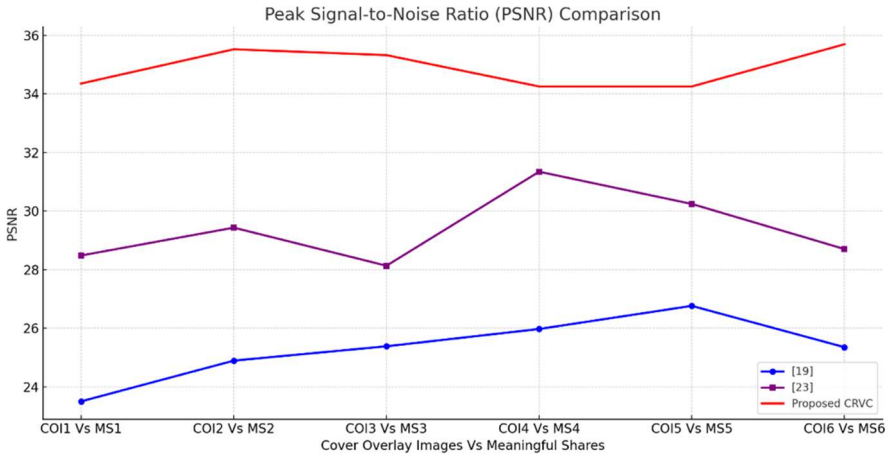
Lower MSE values indicate better performance. Figure 9 shows that the Proposed CRVC method consistently shows the lowest MSE across all cases. Higher PSNR values indicate better performance. Again, the Proposed CRVC method exhibits the highest PSNR values for most cases. Higher SSIM values (closer to 1) indicate better performance. The Proposed CRVC method shows the highest SSIM values in all cases, with the exception of COI4 Vs MS4 and COI5 Vs MS5, where it is slightly behind or at par with other methods. Similarly, the quality of the RCSC is compared with the CSC across four different sample test images: Eye Biometric, Aadhaar PII (Personally Identifiable Information), Thumb Biometric, and Sensitive Details. The results are tabulated in Table 3.

In light of these performance metrics, it is evident that the proposed CRVC method excels in preserving the quality of the data across different biometric and sensitive details. Remarkably, there is no data loss during the processing phase, and the metrics attest to the accuracy of the reconstruction. Most importantly, this high level of data fidelity is achieved without compromising security. The method maintains the integrity and confidentiality of the data, making it a robust and reliable choice

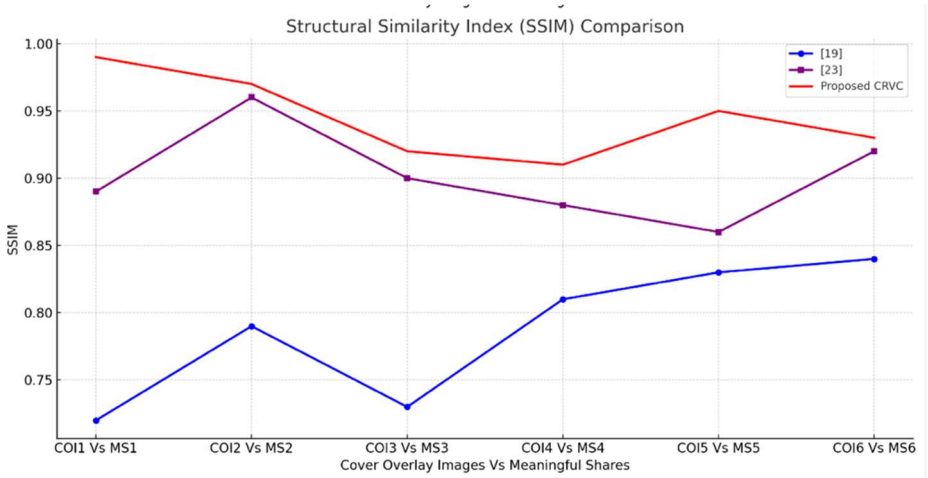
for applications requiring high security and quality. Therefore, the proposed CRVC method offers a significant advancement over traditional methods, particularly in applications that demand high-quality data reconstruction and stringent security measures.



(a) Mean Square Error (MSE) Comparison



(b) Peak Signal-to-Noise Ratio (PSNR) Comparison



(c) Structural Similarity Index (SSIM) Comparison

Figure 9. Quality metrics of meaningful shares.

Table 3. CRVC Performance with integrity verification.

CSC Vs RCSC	Performance Metrics		
	MSE	PSNR	UIQI
(a) Eye Biometric	0	+ Inf dB	1
(b)Aadhaar PII	0	+ Inf dB	1
(c) Thumb	0	+ Inf dB	1
(d) Sensitive details	0	+ Inf dB	1

4.2.3. Comparative analysis

The primary objective of conducting a computational analysis is to assess the efficiency and scalability of the CRVC algorithm. The computational analysis of the proposed CRVC is compared with the existing methods and are tabulated in Table 4. This analysis is vital for determining its applicability in real-world scenarios, mainly where computational resources may be limited or expensive. Additionally, this analysis aims to compare CRVC's computational performance against existing methods to highlight its advantages.

Table 4. Computational performance of proposed CRVC vs. existing methods.

Operations (per pixel)	[11]	[21]	CRVC
Integer Addition	30 to 226	3	2
Integer Subtraction	Nil	1	1
Integer Multiplication	7	Nil	3
Integer Division	5	2	4
Mod	Nil	2	2
Execution Time (Seconds)	2.9 to 6.8	0.5 to 1.1	0.4 to 0.8

Table 5. Feature analysis of proposed CRVC vs. Existing methods.

Features	[11]	[21]	CRVC
Image type	Grayscale	Grayscale	Color
Stacking type	Digital	Digital	Digital
Share type	Random	Meaningful	Meaningful
Authentication by	Additional share	Integrated	Integrated
Verification type	Authentication	Integrity	Integrity
Computational cost	High	Low	Low
Quality of the reconstructed image	Low	High	High

From Table 4, the analysis shows CRVC significantly outperforms existing methods. It takes less time for both the share construction and revealing phases, translating into lower computational costs. The computational analysis confirms that CRVC meets its objective of reducing computational costs without compromising security [31,32]. This analysis establishes CRVC as not only a secure but also an efficient algorithm suitable for a variety of applications, including those that are resource-sensitive.

The feature analysis aims to provide a comprehensive understanding of the functionalities and capabilities of the CRVC, especially in comparison with existing methods. The objective is to evaluate how well CRVC satisfies essential criteria like digital stacking, meaningful sharing, integrity verification, and overall computational efficiency which are tabulated in Table 5.

Table shows that the proposed CRVC exhibits superiority across multiple features. It supports digital stacking and produces meaningful shares, unlike many existing methods. Most importantly, it provides an integrity verification feature, a capability not commonly found in existing solutions. In terms of computational cost and the quality of the reconstructed image, CRVC scores highly, making it a well-rounded solution. Feature analysis shows that CRVC successfully meets its objective of providing a secure and efficient visual cryptographic scheme with an emphasis on integrity verification. The analysis also indicates that CRVC could be more widely applicable than existing methods, especially in high-security areas such as healthcare, finance, and defence. In summary, both Computational and Feature Analyses indicate that CRVC achieves and excels in meeting its objectives, standing out as a more comprehensive solution than existing methods.

Some potential limitations of the proposed methodology is identified and these limitations provide areas for further research and improvement, they don't negate the significant advancements and benefits that OMTAP brings to the field of secure image communication.

Participant Tampering: The methodology is restricted in its ability to verify the integrity of the decoded image if any of the authorized participants intentionally alter their share.

Limited to Grayscale Images: The OMTAP is primarily designed for grayscale secret images and may not be directly applicable or optimized for color or high-dimensional images.

Dependence on Cover Images: The security and efficiency of the method rely significantly on the chosen color cover images. Inefficient or inappropriate selection of cover images can compromise the efficacy of the encryption and decryption processes.

Computational Overhead: While OMTAP aims to be efficient, the multi-tiered authentication process and the generation of asymmetric key matrices could introduce computational overhead, especially for large-sized images [32].

Requirement of All Shares for Decryption: The method necessitates the availability of all shares for successful decryption. If even one share is lost or becomes inaccessible, the secret image may not be retrievable.

No Third-Party Verification: The absence of a third-party verification mechanism might be seen as a limitation in scenarios where external validation is desirable or necessary [33].

The promising results engendered by CRVC on color images posits a fertile ground for extending the protocol to other image types such as Binary and Grayscale images. Future studies may delve into tailoring the CRVC for these image categories, evaluating its performance and identifying any requisite optimizations. Additionally, the incorporation of multiple secret images within a single cryptographic protocol is a captivating avenue for future work. This extension could potentially amplify the security and application spectrum of visual cryptography, making it a more versatile tool in the broader realm of secure digital communication. The anticipated advancements in visual cryptographic protocols, including CRVC, are poised to significantly contribute to the fortification of digital information exchange, particularly in the logistics and supply chain sectors, which are becoming increasingly reliant on image-based document transmission.

5. Conclusions

The secure transmission of image-based documents is an emerging concern in the field of logistics and supply chain management. As businesses continue to adopt new technologies, it's imperative to address the vulnerabilities that come with digital transformation. In the ever-evolving domain of visual cryptography, the need for robust, efficient, and trustworthy methods has never been more pertinent. This research introduced and thoroughly evaluated the CRVC, aiming to address the existing gaps in the field, particularly concerning color image encryption. The CRVC was designed with a clear emphasis on enhancing security, ensuring the integrity of encrypted content, and optimizing computational costs. Through comprehensive analyses, CRVC demonstrated a remarkable capability to encrypt and decrypt color images efficiently, ensuring that the integrity of the original content remains uncompromised throughout the process. Comparative assessments against existing methods further reinforced the efficacy of CRVC. CRVC showcases a superior computational performance, and especially the integrity verification, set it apart from traditional visual cryptographic protocols. Furthermore, the algorithm's adaptability to different image types and sizes, coupled with its resilience against attacks, cements its potential for widespread applications.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Conflict of interest

The authors declare there is no conflict of interest.

References

1. A. Akanksha, H. Garg, S. Shivani, Privacy protection of digital images using watermarking and QR code-based visual cryptography, *Adv. Multimedia*, **2023** (2023), 6945340. https://doi.org/10.1155/2023/6945340
2. M. Naor, A. Shamir, Visual cryptography, *Adv. Cryptol. EUROCRYPT*, **94** (1995), 1–12.
3. F.Aswad, I. Salman, S. Mostafa, An optimization of color halftone visual cryptography scheme based on bat algorithm, *J. Intell. Syst.*, **30** (2021), 816–835.https://doi.org/10.1515/jisys-2021-0042
4. A. J. Blesswin, G. S. Mary, S. M. Kumar, Secured communication method using visual secret sharing scheme for color images, *J. Int. Technol.*, **22** (2021), 803–810. https://jit.ndhu.edu.tw/article/viewFile/2544/2562
5. E. Çiftci, E. Sümer, A novel steganography method for binary and color halftone images, *Peer J. Comput. Sci.*, **8** (2022), 1062. https://doi.org/10.7717/peerj-cs.1062
6. G. S. Mary, A. J. Blesswin, S. M. Kumar, Self-authentication model to prevent cheating issues in grayscale visual secret sharing schemes, *Wirel. Pers. Commun.*, **125** (2022), 1695–1714. https://doi.org/10.1007/s11277-022-09628-8

7. G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, Extended capabilities for visual cryptography, *Theor. Comput. Sci.*, **250** (2001), 143–161. https://doi.org/10.1016/S0304-3975(99)00127-9
8. I. F. Elashry, O. S. Faragallah, A. M. Abbas, S. El-Rabaie, 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.*, **21** (2012), 193–205. https://doi.org/10.1080/19393555.2011.654319
9. J. L. Sian, H. C. Wei, A probabilistic model of visual cryptography scheme with dynamic group, *IEEE Trans. Inf. Forensics Secur.*, **7** (2012), 197–207. https://doi.org/10.1109/TIFS.2011.2167229
10. C. C. Lin, W. H. Tsai, Visual cryptography for gray-level images by dithering techniques, *Pattern Recognit. Lett.*, **24** (2003), 349–358. https://doi.org/10.1016/S0167-8655(02)00259-3
11. A. J. Blesswin, P. Visalakshi, Optimal visual secret sharing on electrocardiography images for medical secret communications, *Int. J. Control Theory Appl.*, **9** (2016), 1055–1062.
12. A. J. Blesswin, G. S. Mary, Optimal grayscale visual cryptography using error diffusion to secure image communication, *Int. J. Control Theory Appl.*, **8** (2015), 1511–1519. https://api.semanticscholar.org/CorpusID:212442311
13. A. J. Blesswin, G. S. Mary, S. M. M. Kumar, Multiple secret image communication using visual cryptography, *Wirel. Pers. Commun.*, **122** (2022), 3085–3103. https://doi.org/10.1007/s11277-021-09041-7
14. Z. Wang, G. R. Arce, Halftone visual cryptography via error diffusion, *IEEE Trans. Inf. Forensics Secur.*, **4** (2009), 383–396. https://doi.org/10.1109/TIFS.2009.2024721
15. G. S. Mary, S. M. M. Kumar, Secure grayscale image communication using significant visual cryptography scheme in real-time applications, *Multimed. Tools Appl.*, **79** (2020), 10363–10382. https://doi.org/10.1007/s11042-019-7202-7
16. A. J. Blesswin, P. Visalakshi, A novel visual image confirmation (VIC) protocol using visual cryptography for securing ubiquitous bluetooth mobile communications, *Res. J. Appl. Sci.*, **9** (2014), 503–510. https://dx.doi.org/10.36478/rjasci.2014.503.510
17. J. S. Pan, T. Liu, H. M. Yang, B. Yan, Visual cryptography scheme for secret color images with color QR codes, *J. Vis. Commun. Image Represent.*, **82** (2021), 103405. https://doi.org/10.1016/j.jvcir.2021.103405
18. R. Wu, S. Gao, X. Wang, S. Liu, Q. Li, U. Erkan et al. AEA-NCS: An audio encryption algorithm based on a nested chaotic system, *Chaos Solitons Fractals*, **165** (2022), 112770. https://doi.org/10.1016/j.chaos.2022.112770
19. Y. Guo, X. Jia, Q. Chu, D. A. Wang, Novel XOR-based threshold visual cryptography with adjustable pixel expansion, *Appl. Sci.*, **10** (2020), 1321. https://doi.org/10.3390/app10041321
20. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, X. Tang, EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory, *Inf. Sci.*, **621** (2023), 766–781. https://doi.org/10.1016/j.ins.2022.11.121
21. G. S. Mary, S. M. Kumar, A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication, *Meas. Sci. Technol.*, **30** (2019), 125404. https://doi.org/10.1088/1361-6501/ab2faa
22. D. Zhang, L. Ren, M. M. Shafiq, Z. Gu, A privacy protection framework for medical image security without key dependency based on visual cryptography and trusted computing, *Comput. Intell. Neurosci.*, **2023** (2023), 6758406. https://doi.org/10.1155/2023/6758406

23. A. J. Blesswin, P. Visalakshi, A new semantic visual cryptographic protocol (SVCP) for securing multimedia communications, *Int. J. Soft Comput.*, **10** (2015), 175–182. https://dx.doi.org/10.36478/ijscomp.2015.175.182
24. S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, et al., Asynchronous updating Boolean network encryption algorithm, *IEEE Trans. Circuits Syst. Video Technol.*, **33** (2023), 4388–4400. https://doi.org/10.1109/TCSVT.2023.3237136
25. N. Rani, S. R. Sharma, V. Mishra, Grayscale and colored image encryption model using a novel fused magic cube, *Nonlinear Dyn.*, **108** (2022), 1773–1796. https://doi.org/10.1007/s11071-022-07276-y
26. S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, et al., A 3D model encryption scheme based on a cascaded chaotic system, *Signal Process.*, **202** (2023), 108745. https://doi.org/10.1016/j.sigpro.2022.108745
27. Q. Lai, L. Yang, G. Chen, Design and performance analysis of discrete memristive hyperchaotic systems with stuffed cube attractors and ultraboosting behaviors, *IEEE Trans. Ind. Electron.*, **2023** (2023), 1–10. https://doi.org/10.1109/TIE.2023.3299016.
28. D. R. Somwanshi, V. T. Humbe, A secure and verifiable color visual cryptography scheme with LSB based image steganography, *Int. J. Adv. Trends Comput. Sci. Eng.*, **10** (2021), 2669–2677. https://doi.org/10.30534/ijatcse/2021/031042021
29. Q. Lai, Z. Wan, H. Zhang, G. Chen, Design and analysis of multiscroll memristive hopfield neural network with adjustable memductance and application to image encryption, *IEEE Trans. Neural Networks Learn. Syst.*, **34** (2023), 7824–7837. https://doi.org/10.1109/TNNLS.2022.3146570
30. X. Wu, C. N. Yang, Probabilistic color visual cryptography schemes for black and white secret images, *J. Vis. Commun. Image Represent.*, **70** (2020), 102793. https://doi.org/10.1016/j.jvcir.2020.102793
31. C. N. Yang, L. Z. Sun, S. R. Cai, Extended color visual cryptography for black and white secret image, *Theor. Comput. Sci.*, **609** (2016), 143–161. https://doi.org/10.1016/j.tcs.2015.09.016
32. Q. Lai, Z. Wan, P. D. K. Kuate, Generating grid multi-scroll attractors in memristive neural networks, *IEEE Trans. Circuits Syst.*, **70** (2023), 1324–1336. https://doi.org/10.1109/TCSI.2022.3228566
33. Q. Lai, Z. Chen, Grid-scroll memristive chaotic system with application to image encryption, *Chaos Solitons Fractals*, **170** (2023), 113341. https://doi.org/10.1016/j.chaos.2023.113341

AIMS Press