A Narrative Study on Visual Cryptography Techniques for Robust and Secure Image Communication: A Review

Shibani Raju S and Dr. John Blesswin A

ABSTRACT

Visual cryptography is a powerful method for securely sharing and protecting visual data by splitting an image into multiple shares. Individual shares do not reveal any information, but when combined, they allow for the reconstruction of the original image. The survey categorizes different approaches based on pixel expansion, complexity, and the quality of the reconstructed image. It focuses specifically on color image encryption, an emerging field of interest because of its use in secure communication, digital media, and medical imaging. The paper provides a comprehensive review of recent advances in color visual cryptography, discussing the latest techniques and challenges in the field. his paper is a systematic review of color visual cryptography techniques. The contribution is threefold: (i) categorizing schemes by pixel expansion, complexity, and reconstruction quality, (ii) critically analyzing limitations and trade-offs, and (iii) identifying open research gaps and future directions.

Keywords: Color visual cryptography, Share generation schemes, Pixel expansion optimization, Color image secret sharing, Reconstructed image quality metrics

Research Scholar, Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu, India ROR

Correspondence to:
Shibani Raju S,
sr2396@srmist.edu.in

Additional material is published online only. To view please visit the journal online.

Cite this as: Shibani Raju S and Blesswin J. A Narrative Study on Visual Cryptography Techniques for Robust and Secure Image Communication: A Review. Premier Journal of Science 2025;15:100156

DOI: https://doi.org/10.70389/PJS.100156

Peer Review

Received: 14 August 2025

Last revised: 8 October 2025

Accepted: 8 October 2025

Version accepted: 3

Published: 24 December 2025

Ethical approval: N/a

Consent: N/a

Funding: No industry funding

Conflicts of interest: N/a

Author contribution:
Shibani Raju S and John Blesswin A – Conceptualization, Writing – original draf, review and editing

Guarantor: Shibani Raju S

Introduction

Image communication is the act of exchanging images among applications and systems. Image communication can be represented by integrity, confidentiality, and authentication. In the contemporary digital world, image communication has been a highly effective tool for communicating complex ideas quickly. Visual information, such as images, infographics, and diagrams, acts as a universal language that helps people from different backgrounds understand messages easily without relying on text. It also facilitates real-time comprehension, and so it is an essential tool for applications across education to marketing. Image communication is important as it facilitates quick and transparent communication of advanced information, transcending linguistic boundaries, and augmenting comprehension. Visual Cryptography (VC) is a method that divides a secret image into several shares or transparencies, where each share individually contains no information about the original image. The entire image can be reconstructed only by combining the shares. For encryption, the original image is divided into several shares. For example, when an image is divided into two shares, each pixel from the original image is split into two corresponding pixels in the shares. One pixel in each share is randomly assigned, while the other is calculated so that the original pixel becomes visible when the shares are layered together. For decryption, to view the original image, the shares are stacked or overlaid. The visual information from each share combines to reveal the original image. This process ensures secure image transmission, maintaining confidentiality and preventing unauthorized access during communication.

Review Methodology

This systematic review adheres to established guidelines to guarantee thorough coverage of visual cryptography research. A systematic search was performed across various academic databases, including IEEE Xplore, ACM Digital Library, Springer, and Google Scholar, utilizing key terms such as “visual cryptography,” “color image encryption,” “secret sharing schemes,” and “visual secret sharing.” The review included literature from 2000 to 2024 to document the progression of techniques from foundational studies to modern developments. The inclusion criteria emphasized peer-reviewed articles, conference proceedings, and book chapters that specifically addressed methods of color visual cryptography, while excluding non-English publications, abstract-only papers, and studies restricted to binary or grayscale images. The initial search produced around 150 papers, which were systematically screened for relevance based on titles and abstracts, followed by a full-text evaluation for final selection. The screening process yielded 30 high-quality papers that fulfilled all inclusion criteria and exhibited substantial contributions to the field of color visual cryptography research. The data extraction emphasized methodology, performance metrics, pixel expansion factors, computational complexity, and reconstructed image quality to facilitate a thorough comparative analysis of various approaches.

Basic of Visual Cryptography

VC is a cryptographic method used to secure images by splitting them into multiple shares. At its simplest level, which is referred to as VC (2,2) , an image is split into two shares.[1] A pixel from the original image is split into two sub-pixels, and each is distributed randomly to the two shares. On their own, these shares look like random patterns and reveal nothing about the original image. However, when the two shares are stacked, the original image is reconstructed and becomes visible. This method is particularly useful for secure image sharing and authentication, where the original image can exclusively be revealed by the intended recipient possessing all necessary shares. The strength of VC lies in its simplicity, as it doesn’t require complex algorithms to decrypt the image, only the proper stacking of shares. Additionally, the method offers strong resistance against brute-force and statistical attacks, ensuring human-perceptible visual recovery without

Provenance and peer-review:
Unsolicited and externally peer-reviewed

Data availability statement:
The authors confirm that the data supporting the findings of this study are available in the article

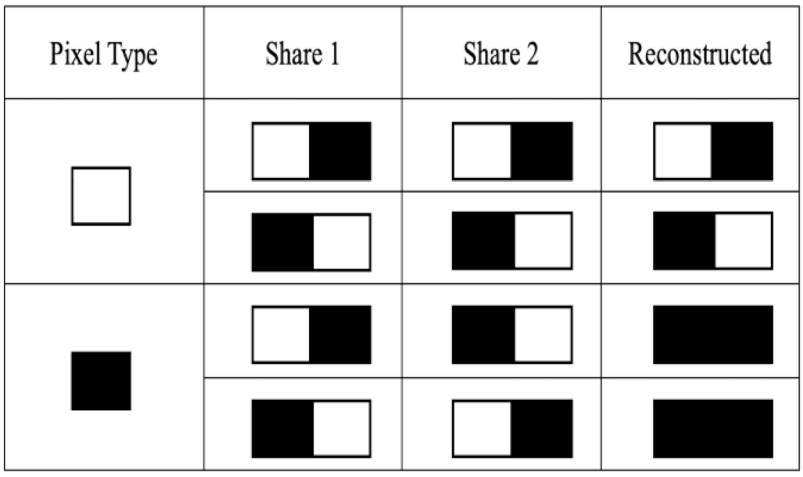

Fig 1 | Pixel representation of Naor and shamir scheme

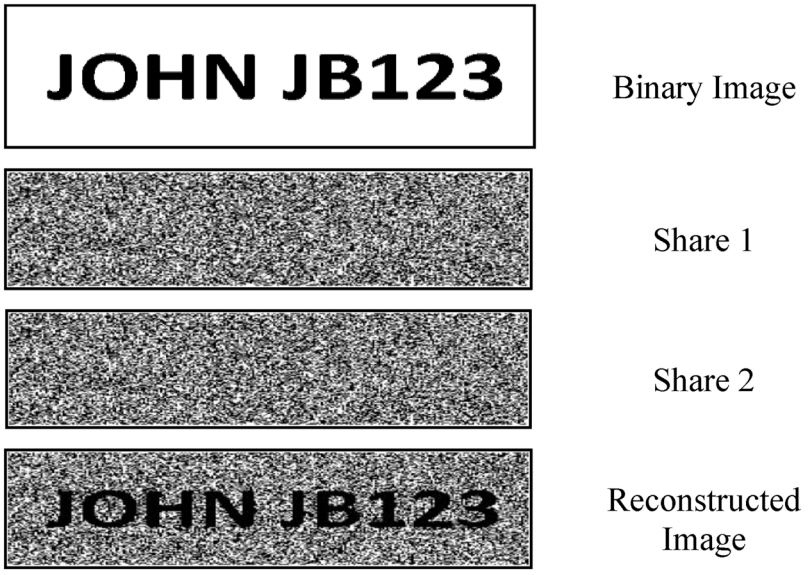

Fig 2 | Pixel representation of Naor and shamir scheme

the need for computational decryption or cryptographic keys. Moreover, modern VC approaches integrate visual quality enhancement and pixel optimization techniques to improve the clarity and contrast of the reconstructed image.

Figure 1 illustrates a simple VC scheme used to securely share a secret image between two participants. The Naor and Shamir Scheme,[31] introduced in 1994, is one of the earliest and most influential techniques in Visual Cryptography, enabling secure image sharing by dividing a secret image into multiple shares, each appearing as random noise when viewed individually. Only when these shares are overlaid does the original image become visible, without requiring any complex computation or decryption algorithm. In this scheme, every pixel of the secret image—either black or white—is divided into two sub-pixels distributed across two separate shares, referred to as Share 1 and Share 2. For a white pixel, Share 1 contains one white and one black sub-pixel, while Share 2 contains the reverse pattern, whereas for a black pixel, both shares carry the same sub-pixel arrangement, either black–white or white–black, depending on the encoding pattern used. When the two shares are superimposed, the human visual system perceives the reconstructed image: white pixels appear lighter or grayish due to alternating sub-pixels, while black pixels appear completely dark. This ensures that neither of the individual shares reveals any information about the original secret, thereby maintaining complete confidentiality until both shares are combined. Furthermore, this method is classified as a (2,2) Visual Cryptography Scheme, indicating that both shares are required for decryption, and the reconstruction process relies entirely on human visual perception rather than computational processing. This approach provides a high level of security since no partial information can be extracted from a single share; however, it introduces the limitation of pixel expansion, where each pixel of the original image is represented by multiple sub-pixels in the shares, leading to an increase in image size. Despite this drawback, the Naor and Shamir scheme remains a foundational technique in the field of Visual Cryptography, serving as the basis for advanced methods such as Color Visual Cryptography, Progressive VC, and Meaningful Share Generation. In practical applications, this scheme is widely utilized in secure image transmission, confidential document sharing, and biometric authentication systems, where data privacy and visual integrity are of critical importance. Additionally, recent studies have optimized this scheme by reducing pixel expansion and improving image contrast for better visual quality. It also forms the basis for hybrid models that integrate computational cryptography with VC to enhance security levels.

Figure 2 shows the VC process applied to a binary image containing text. The process starts with the original binary image, where the text is easily readable in black on a white background. This image is split into two distinct shares, referred to as “Share 1” and “Share 2.”

DOI: https://doi.org/10.70389/PJS.100156 | Premier Journal of Science 2025;15:100156

Table 1 | Analysis of COLOR visual cryptography techniques

Authors	Pixel Expansion	Complexity	Methodology	Reconstructed Image Quality	PSNR
[1]	1	High	A Thumbnail Preserving Encryption (TPE) scheme.	Low	28.4
[2]	1	High	Color Secret Sharing Protocol (CSSP)	High	34.7
[3]	1	High	Elzaki transformation and substitution.	Medium	30.2
[4]	1	High	A four-dimensional (4D) hyperchaotic Chen map and a hybrid DNA coding	Medium	31.5
[5]	2	High	Shamir scheme with the Cipher Block Chaining (CBC) mode of operation.	High	35.9
[6]	2	High	Harris Hawks Optimization (HHO) algorithm.	Low	26.8
[7]	1	High	New approach based on an evolutionary framework.	High	33.1
[8]	1	High	A cryptanalysis driven design approach is used.	Low	27.6
[9]	1	High	Jarvis halftoning is used.	High	36.4
[10]	2	High	Encrypted by four shares cyan, magenta, yellow, mask	Medium	29.3
[11]	1	High	Arnold transform and pixel vectorization.	High	34.1
[12]	2	High	Four different encoding modes (numeric, alphanumeric, kanji, binary).	High	35.0
[13]	2	High	Hybrid VC algorithm.	Medium	30.7
[14]	1	High	Rivest Shamir Adleman (RSA) algorithm and the Gaussian pyramid (GP)	Low	27.2
[15]	1	High	Hybrid substitution cryptographic methods with Vigenere & Beaufort method	High	34.6
[16]	1	High	Blowfish algorithmic rule	High	32.8
[17]	1	High	Image feature protection techniques to conventional image retrieval techniques.	Low	25.9
[18]	1	High	Adaptive halftoning technique	High	33.4
[19]	1	High	Halftone Visual Cryptography (HVC) construction method.	High	35.6
[20]	1	High	Normal cryptographic techniques.	Medium	30.1
[21]	3	High	Embedded Extended VC using Artificial Bee Colony (ABC).	Medium	29.8
[22]	1	High	A New dual watermarking.	High	34.9
[23]	1	High	A new color VC scheme.	High	36.0
[24]	1	High	A two-tier protection mechanism for Dual Modular Redundancy (DMR).	High	33.5
[25]	1	High	Images are halftoned and encrypted using a binary key image through an XOR	High	34.3
[26]	2	High	Visual information pixel (VIP) synchronization and error diffusion.	Low	26.5
[27]	1	High	Halftoning technique and error diffusion techniques.	Medium	29.6
[28]	1	High	A shared key algorithm that in the Joint Photographic Experts Group (JPEG) domain.	Low	25.7
[29]	1	High	Canonical schemes.	Low	27.9
[30]	1	High	Simple algorithms on two camouflage.	Medium	30.9

Both shares are random noise, and contain no apparent pattern or information that can be seen by the naked eye. This randomness guarantees that each share separately cannot disclose the content of the original image. But, when the two shares are overlap or added together, the original text is reconstructed in the "Reconstructed Image" portion. The reconstructed image appears slightly blurred, with some areas looking less sharp or mixed in gray shades as a result of the overlap of black and white sub-pixels from the two shares. This method safely conceals the data, since only when both the shares are used together can they be disclosed, proving the utility of VC to secure sensitive visual information.

Types of Visual Cryptography

Before Types of VC, it is important to understand the various methods and schemes developed to encode visual information into multiple shares that can only be decoded when the appropriate shares are combined. These types differ in terms of how they handle images, the number of shares required for reconstruction, the complexity of the encryption, and the quality of the reconstructed image. Each type is designed to balance security, visual quality, and computational efficiency based on application needs. Additionally, some schemes focus on reducing pixel expansion to minimize storage and transmission overhead, while others aim to support color images, grayscale images, or even meaningful shares that reveal partial information without compromising the full secret.

Figure 3 illustrates the different types of VC schemes based on the nature of the secret image representation. VC techniques are broadly categorized into three types Binary, Grayscale, and Color depending on the pixel characteristics and visual information used during encryption and decryption.

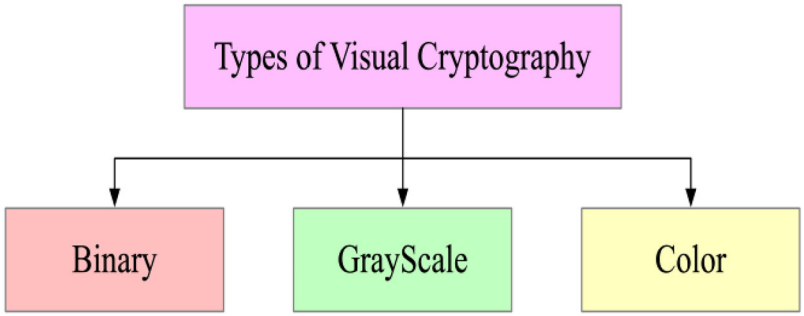

Fig 3 | Classification of visual cryptography techniques

Binary Image Cryptography

A binary image is composed of pixels that can take on only two possible colors, typically black and white. These images are usually presented in black and white, where the two pixel values are commonly represented as 0 for black and either 1 or 255 for white.

Grayscale Image Cryptography

A Grayscale image only contains luminance information and no color information. The contrast extends from Black to white in its strongest intensity.

Color Image Cryptography

A Color image is used to characterize the colors interns of intensity values. In the case of classical color images, this domain is then brought down to three channels, each corresponding to the primary color: red, green and blue.

Review of Visual Cryptography: Methodologies, Outcomes, and Research Trends

This section provides a detailed analysis of various VC techniques, based on a review of 30 research papers. The analysis is structured into two key tables: one focuses on Methodology and Outcomes, and the other on Research Characteristics.

Methodology and outcomes in color visual cryptography

Methodology and Outcomes examines four critical parameters: pixel expansion, computational complexity, methodology, and the reconstructed image's quality. These factors are essential for assessing the effectiveness and efficiency of different VC techniques

Table I reviews the different VC techniques with respect to four key parameters: pixel expansion, complexity, methodology, and reconstructed image quality.

Pixel Expansion refers to the increase in the number of pixels after the encryption process, which can affect the efficiency and applicability of the encryption algorithm. Pixel expansion values in this table are normally low (1) or medium (2), with one having a high expansion (3). Low pixel growth typically signifies a more efficient system that does not increase image size much, whereas higher values can signify more detailed or complicated encryption. High pixel expansion can affect storage and transmission needs, so it is important to strike a balance between security requirements and resource limitations.

Complexity assesses how computationally intensive the encryption process. All the methods listed in the table are marked as high in complexity, which suggests that they require significant computational resources. This high complexity is often associated with advanced encryption algorithms or the integration of multiple cryptographic techniques.

Methodology refers to the specific cryptographic or transformation techniques used in the encryption process. The table lists a diverse range of methodologies, from simple substitution and permutation schemes to more complex approaches involving hyperchaotic maps, DNA coding, and adaptive halftoning. For example, Yongming Zhang[1] utilize a transformation and permutation encryption scheme, while Wassim Alexan[4] employ a four-dimensional hyperchaotic Chen map combined with DNA coding, demonstrating the wide variety of approaches taken to enhance security.

Reconstructed Image Quality indicates the visual quality of the image after decryption. High-quality reconstructed images are crucial in applications like medical imaging, where clarity and accuracy are essential. The table shows a mix of high, medium and low image qualities, with high quality results being more desirable but often requiring more sophisticated or complex methodologies. The reconstructed image quality in VC refers to how accurately the original secret image is revealed when the shares are combined. This quality can vary based on the specific VC scheme used, the pixel expansion factor, and how the shares are generated and overlaid. The quality is typically categorized into three levels: Low, Medium, and High.

In low-quality reconstruction, the secret image is visible when the shares are combined, but the clarity and sharpness are significantly reduced. The image may appear blurry, pixelated, or have substantial noise, making fine details hard to discern. In medium-quality reconstruction, the secret image is reasonably clear but may still lack some fine details and sharpness. The image is recognizable, but minor artifacts or noise might be present. In high-quality reconstruction, the secret image is revealed with great clarity and sharpness. The image closely resembles the original, with minimal loss of detail and little to no noise. For instance, Suresh Sankaranarayanan.[2] CSSP achieves high reconstructed image quality, whereas Yongming Zhang.[1] TPE scheme results in low image quality.

Advances in secure visual cryptography

The various approaches discussed in these works focus on enhancing security and quality in VC and image encryption, particularly in the transmission and storage of medical and digital images. Techniques such as semantic preservation and complete cross-plane protection[1] and chaotic systems in an evolutionary framework[7] are integrated with cryptographic methods like Shamir's secret sharing, Advanced Encryption Standard (AES) encryption,[4] and Deoxyribonucleic acid (DNA) coding[4] to achieve higher security. The use of hybrid methods,

DOI: https://doi.org/10.70389/PJS.100156 | Premier Journal of Science 2025;15:100156

Table 2 | Characteristics of COLOR visual cryptography techniques

Authors	Year	Type of Shares Generated	Type of Secret Image	No. of Secret Images	No. of Share Image
[1]	2024	Meaningful	Color	1	3
[2]	2024	Meaningful	Color	4	3
[3]	2024	Meaningful	Color	2	2
[4]	2023	Random	Color	2	2
[5]	2023	Random	Color	1	3
[6]	2023	Random	Color	1	2
[7]	2023	Random	Color	1	1
[8]	2023	Random	Color	4	1
[9]	2023	Random	Color	1	4
[10]	2022	Random	Color	1	4
[11]	2022	Meaningful	Color	3	3
[12]	2022	Random	Color	2	1
[13]	2021	Meaningful	Color	6	1
[14]	2021	Meaningful	Color	4	1
[15]	2020	Random	Color	1	2
[16]	2019	Random	Color	1	1
[17]	2018	Meaningful	Color	4	4
[18]	2017	Meaningful	Color	3	2
[19]	2016	Meaningful	Color	2	2
[20]	2015	Meaningful	Color	1	1
[21]	2014	Meaningful	Color	2	2
[22]	2013	Meaningful	Color	2	2
[23]	2013	Random	Color	4	3
[24]	2012	Meaningful	Color	1	1
[25]	2011	Random	Color	1	2
[26]	2011	Meaningful	Color	2	2
[27]	2009	Random	Color	4	2
[28]	2005	Random	Color	3	2
[29]	2003	Random	Color	2	2
[30]	2000	Meaningful	Color	2	2

such as combining Vigenere and Beaufort encryption[15] further improves image quality and robustness against attacks. Advanced algorithms like the ABC[21] and HHO[6] also contribute to reducing complexity and avoiding pixel expansion. These methods address limitations such as color distortion and pixel expansion, ensuring lossless recovery. The focus on preserving image quality while enhancing security, especially through innovative techniques like shared key encryption in the JPEG domain[28] and robust watermarking,[21] illustrates the continuous evolution in the field of VC and image encryption.

Critical analysis of current limitations

A trade-off is evident across visual cryptography techniques: methods with low pixel expansion, such as,[1,2] improve efficiency but often compromise on security, whereas higher expansion schemes like[21] strengthen protection at the cost of storage overhead. Performance gaps also remain, as high-quality reconstruction methods[2,7,9] typically rely on meaningful shares, making them more vulnerable to visual attacks compared to random-share approaches. Despite nearly all schemes reporting "high complexity," standardized computational time comparisons are absent, limiting clarity on real-world deployment. Moreover, no existing method achieves the ideal combination of pixel expansion = 1 with consistently high reconstruction quality, leaving this as an open research challenge. Finally, share generation strategies impact practicality: multi-share approaches[1,5,9] pose storage and transmission issues for mobile or IoT contexts, while single-share models,[7,16] fall short of security requirements in sensitive applications.

Challenges in Visual Cryptography Complexity

The system's complexity and computational demands create significant obstacles to its scalability and efficiency, particularly with larger images or complex datasets. Despite a modest improvement in the quality of reconstructed images, the associated increase in computational costs outweighs the benefits. Consequently, the system is not well-suited for real-time or resource-constrained environments. The intricate processes involved, including halftoning and error diffusion, further limit its practicality. Moreover, the high memory requirements and processing overhead make it challenging to integrate with lightweight devices such as IoT sensors and edge computing nodes. Optimizing the algorithm for parallel processing could help mitigate some of these challenges (Table 2).

Research characteristics:

The Research Characteristics table explores four parameters as well: the types of shares generated, the nature of the secret image, the number of secret images, and the number of share images. These aspects highlight the diverse approaches and configurations used in the field. Finally, the overall advancements and challenges in VC methods are discussed, providing insights into the current state and future directions of this research area. The table outlines the characteristics of various VC methods based on several key parameters: authorship, year of publication, type of shares generated, type of secret image, number of secret images, and the number of share images. Authorship and Year indicate who developed each technique and when it was published. This provides a timeline of advancements in VC from 2000 to 2024, showing how methods have evolved over time. For instance, early works by Chin-Chen Chang[27] in 2000 and 2009 laid foundational concepts that later researchers, like Yongming Zhang[1] and Suresh[2], have built upon in 2024.

Type of Shares Generated is categorized into "Meaningful" and "Random" shares. Meaningful shares, also known as structured or visually significant shares, are designed to look like meaningful images, even when they are viewed individually. These shares are often used in scenarios where each share needs to be visually appealing or convey some information, even when

the secret cannot be revealed without combining them. Each share has a meaningful appearance, such as a recognizable image or pattern, even when viewed on its own. When the shares are overlaid, they still reveal the secret image. This approach is often used in applications where the shares need to carry some visual significance or where random noise patterns are undesirable. The trade-off is typically a reduction in security compared to random shares, as the structure of the shares might provide some clues about the secret. In a meaningful share scheme, two images might be generated where one is a picture of a cat and the other is a picture of a dog. Neither image on its own reveals the secret, but when combined, they might reveal a hidden message or another image.

Random shares are composed of random pixel patterns. When you look at each share individually, they appear as random noise with no discernible information. This randomness ensures that no information about the secret is revealed until the shares are combined. Each share looks like a completely random pattern of black and white pixels. The individual shares are meaningless on their own. Only when the correct number of shares is overlaid or combined does the original secret image become visible. The security is very high because the random nature of the shares makes it impossible to guess the secret without all necessary shares. If you have a 2-out-of-2 VC scheme, two random-looking images (shares) are generated. Neither image reveals any information, but when they are overlaid, the original secret image is revealed. For example, methods by Yongming Zhang[1] and Bishoy Sharobim[11] generate meaningful shares. On the other hand, random shares appear as noise until properly decrypted, which enhances security but can be less practical for certain uses, as seen in the work of Wassim Alexan[4] and many others.

Type of Secret Image indicates that all the methods listed focus on encrypting color images. This uniformity suggests a common challenge in the field maintaining the integrity and quality of color images during and after the encryption process, which is crucial for applications in areas like medical imaging, secure communications, and digital art.

Number of Secret Images refers to the quantity of original images being encrypted in each method. Most methods focus on encrypting a single secret image, which simplifies the process and is typical in many practical applications. However, some approaches, like those by Suresh Sankaranarayanan[2] and Mohd Amaan Siddiqui[13] deal with multiple secret images (up to six), indicating more complex encryption scenarios that can be beneficial in advanced security applications.

Number of Share Images corresponds to how many images are generated to represent the encrypted secret. The number of share images varies across methods, ranging from 1 to 4. Methods generating fewer shares, like those by Xinpeng Man[7] and Hira Nazir[8] tend to focus on simplifying the decryption process or reducing storage requirements, while methods generating more shares, like those by Somwanshi[9] and Anli Sherine[10] might be aiming for enhanced security or specific application requirements where multiple shares are beneficial.

Key Metrics for Evaluating Visual Share Quality

The visual quality of shares in VC is crucial for determining the effectiveness of the technique. This quality is quantitatively assessed using three key metrics: PSNR (Peak Signal-to-Noise Ratio), MSE (Mean Squared Error), and SSIM (Structural Similarity Index). PSNR and MSE evaluate the fidelity of the shares compared to the original images, while SSIM provides a measure of perceptual similarity, considering structural information and image degradation. These metrics collectively help in understanding how well the visual shares maintain the integrity and appearance of the original image.

Peak Signal-to-Noise Ratio

PSNR is a metric used to assess the quality of a reconstructed or compressed image compared to its original version. It measures how much noise (error) is introduced during compression. A higher PSNR value indicates that the reconstructed image is closer to the original, implying better quality. PSNR is expressed in decibels (dB), calculated using a logarithmic scale, making it more sensitive to small differences in high-quality images.

$$PSNR = 10\left(\frac{MAX^2}{MSE}\right) \tag{1}$$

In equation (1), where MAX is the maximum possible pixel value of the image (e.g., 255 for 8-bit images). MSE is the Mean Squared Error between the original and reconstructed images.[4]

Mean Squared Error (MSE)

MSE measures the average of the squared differences between the original and reconstructed pixel values. A smaller MSE indicates a reduced error, which implies that the reconstructed image is nearer to the original. It calculates the error as the difference between corresponding pixels of the original and reconstructed images.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I(i,j) - K(i,j)\right]^2 \tag{2}$$

In equation (2), where M are the dimensions of the image. *I (i, j)* is the pixel value at position *(i, j)* in the original image. *K (i, j)* is the pixel value at position *(i, j)* in the reconstructed image.[28]

Structural Similarity Index (SSIM)

SSIM estimates the similarity between two images with respect to luminance, contrast, and structure, reflecting perceived changes in structural information. SSIM ranges from −1 to 1, where 1 indicates perfect similarity, indicates no correlation, and negative values indicate dissimilarity. It considers the interdependence of pixel

DOI: https://doi.org/10.70389/PJS.100156 | Premier Journal of Science 2025;15:100156

values in the neighbourhood, unlike PSNR and MSE, which are pointwise measures.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (3)$$

In Equation (3), Where μ_x and μ_y are the average intensities of images x and y. σ_x^2 and σ_y^2 are the variances of x and y. σ_{xy} is the covariance of x and y. C_1 and C_2 are constants to stabilize the division.[23]

Securing Color Images Through Advanced Encryption Methods

A significant number of these papers, especially from 2020 onwards, focus on the encryption and sharing of color images, reflecting a growing trend in enhancing security for more complex and visually rich data. The papers employ a wide range of methodologies, including hybrid substitution ciphers,[15] chaotic systems,[4] genetic codes, Harris Hawks Optimization algorithms,[6] and error diffusion techniques,[26] indicating the variety of approaches being explored to improve the effectiveness and efficiency of color image encryption. Many studies center around VC, particularly for color images, which extend traditional black-and-white VC techniques. The use of color increases the complexity but also enhances applicability in real-world scenarios, especially within intelligent networked environments where secure visual data transmission is crucial.

A common theme is the emphasis on secret sharing schemes, where a secret image is divided into multiple shares that are required to be merged in order to create the original image. This method is important in secure transmission and storage of sensitive visual data, such as 5G-enabled IoT ecosystems and edge computing frameworks. With the increasing interconnectivity of devices, ensuring robust encryption and secure communication channels has become a priority. Several recent studies, such as those using chaotic systems and evolutionary frameworks, highlight the trend of integrating advanced mathematical models and optimization algorithms to improve security and unpredictability. The fusion of VC with machine learning and deep learning-based anomaly detection further strengthens security by enabling adaptive threat response mechanisms. Many studies evaluate their methodologies based on specific performance metrics such as pixel expansion, computational complexity, and the quality of the reconstructed image, indicating a strong focus on quantifiable improvements. Additionally, real-time encryption and decryption processes are being optimized for distributed networks, ensuring minimal latency while maintaining high security levels. Several papers explore practical applications of cryptographic schemes in securing medical images, cloud storage, and IoT devices—domains where intelligent networks play a crucial role in data exchange and processing. There is a noticeable trend towards hybrid techniques, combining multiple cryptographic approaches like chaos theory with genetic algorithms or watermarking with VC to enhance security features and address the limitations of individual methods. The complexity of cryptographic schemes has been increasing, with recent studies integrating more sophisticated algorithms and frameworks, such as fractional-order hyperchaotic maps[4] and multi-level VC, to meet the evolving security challenges in distributed high-speed communication infrastructures.

Conclusion

The paper presents a detailed overview of color VC, with focus on advancements, methodologies, and challenges in the field. It highlights the balance between security and image quality within different cryptographic schemes, particularly in color image encryption. The paper addresses the difficulties in these methods, such as pixel expansion and computational complexity, and investigates hybrid approaches that strive to find balance between security and efficiency. Future advancements are anticipated to further automate secure image sharing with high protection levels. The growing emphasis on improving the quality of reconstructed images while maintaining robust security measures is evident, indicating a significant trend in the development of VC methods for secure communication and data protection.

References

1 Zhang Y, Zhao R, Zhang Y, Yi S, Lan R. Visually semantics-aware color image encryption based on cross-plane substitution and permutation. IEEE Trans Ind Inform. 2024;20(8):10576–86.

2 Sankaranarayanan S, et al. Enhancing healthcare imaging security: Color secret sharing protocol for the secure transmission of medical images. IEEE Access. 2024;12:100200–16. https://doi.org/10.1109/ACCESS.2024.3426935.

3 Mardan A, Shadman R, Al-rassam O. Encryption of color images with a new framework. ARO-Sci J Koya Univ. 2024;12(1):170–80.

4 Alexan W, Gabr M, Mamdouh E, Elias R, Aboshousha A. Color image cryptosystem based on sine chaotic map, 4D Chen hyperchaotic map of fractional-order and hybrid DNA coding. IEEE Access. 2023;11:54928–56.

5 Farran Martín J, Cerezo D. A new color image secret sharing protocol unpublished, 2023. https://doi.org/10.21203/rs.3.rs-3144967/v1

6 Ibrahim DR, Sihwail R, Abuthawabeh A, Abduljabbar M, Mizher A. A novel color visual cryptography approach based on Harris hawks optimization algorithm. Symmetry. 2023;15(7):1305. https://doi.org/10.3390/sym15071305.

7 Song Y. Encryption of color images with an evolutionary framework controlled by chaotic systems. Entropy. 2023;25(4):631. http://doi.org/10.3390/e25040631.

8 Nazir H, Bajwa IS, Abdullah S, Kazmi R, Samiullah M. A color image encryption scheme combining hyperchaos and genetic codes. IEEE Access. 2022;10:14480–95.

9 Somwanshi DR, Humbe VT. Half-tone visual cryptography scheme for RGB color images. Indian J Sci Technol. 2022;16(5):357–66.

10 Sherine A, Peter G, Stonier AA, Praghash K, Ganji V. CMY color spaced-based visual cryptography scheme for secret sharing of data. Wirel Commun Mob Comput. 2022;2022:1–12. https://doi.org/10.1155/2022/6040902

11 Sharobim BK, Abd-El-Hafiz SK, Sayed WS, Said LA, Radwan AG. A secured lossless visual secret sharing for color images using Arnold transform. in Proc. 2022 Int. Conf. Microelectron. (ICM), Casablanca, Morocco, 2022, pp. 254–257, https://doi.org/10.1109/ICM56065.2022.10005395.

12 Bhardwaj C, Garg H, Shekhar S. An approach for securing QR code using cryptography and visual cryptography. In: 2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES); 2022 May 20-21; Greater Noida, India. IEEE; 2022. p. 284–8.

13 Siddiqui MA, Singh K, Saxena A. Multilevel secure multilevel share-based visual cryptography color images for cloud storage. In: 2021 2nd International Conference on Computing

Methods, Science and Technology (ICCMST); 2021 Nov 24-25; Mohali, India. IEEE; 2021. p. 62–7. https://doi.org/10.1109/ICCMST54943.2021.00024.
14 Vishwakarma S, Gupta NK. An efficient color image security technique for IoT using fast RSA encryption technique. In: 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT); 2021 Jun 24-26; Bhopal, India.IEEE; 2021. p. 717–22.
15 Hidajat MS, Setiarso I. Securing digital color image based on hybrid substitution cipher. J Arabic Islamic Stud. 2020;4(2):86–95. https://doi.org/10.33633/JAIS.V4I2.3380
16 Abraham RR, Achenkunju JP, Thomas A, Sekhar GR, Oommen RR. k-n share generation for securing color images using visual cryptography. Int J Eng Res Technol. 2019;5(12):339–43.
17 Arun J, Choudhary R. Image encryption for secure data transfer and image-based cryptography. Int J Eng Res Technol. 2018.
18 Sathishkumar R, Sudha GF. Authenticated color extended visual cryptography with perfect reconstruction. In: 2017 International Conference on Communication and Signal Processing (ICCSP); 2017 Apr 6-8; Chennai, India. IEEE; 2017. p. 609–15.
19 Tiwari S, Sharma N, Gupta N. Analysis of secret share design for color image using visual cryptography scheme and halftone. Int J Comput Appl. 2016;155(13):12–6. https://doi.org/10.5120/IJCA2016912454.
20 Johny S, Antony A. Secure image transmission using visual cryptography scheme without changing the color of the image. In: 2015 IEEE International Conference on Engineering and Technology (ICETECH); 2015 Mar 20; Coimbatore, India. pp. 1–3.
21 Deepa AK, Bento B. Embedded extended visual cryptography scheme for color image using ABC algorithm. In: 2014 12th International Conference on Signal Processing (ICSP); 2014 Oct 19-23; Hangzhou, China. [Place of publication unknown]: IEEE; 2014. p. 653–7.
22 Han Y, Shang Y, He W. DWT-domain dual watermarking algorithm of color image based on visual cryptography. In: Proceedings of the 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing; 2013 Oct 16-18; Beijing, China. IEEE; 2013. p. 373–8.
23 Liu X-Y, Chen M-S, Zhang Y-L. A new color visual cryptography scheme with perfect contrast. In: 2013 8th International Conference on Communications and Networking in China (CHINACOM); 2013 Aug 14-16; Guilin, China. IEEE; 2013. p. 449–54.
24 Malik R, Chugh S. Protection mechanism using cryptography and robust watermarking for color images.
25 Krishnan G, Loganathan D. Color image cryptography scheme based on visual cryptography. In: 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN); 2011 Jul 21-22; Thuckalay, India. IEEE; 2011. p. 404–7.
26 Kang I, Arce GR, Lee H-K. Color extended visual cryptography using error diffusion. IEEE Trans Image Process. 2011 Jan;20(1):132–45.
27 According to Vancouver style, the citation for "Self-verifying visual secret sharing using error diffusion and interpolation techniques" by Chang C-C, Lin C-C, Le THN, and Le HB would be "Chang C-C, Lin C-C, Le THN, Le HB. Self-verifying visual secret sharing using error diffusion and interpolation techniques. IEEE Trans Inf Forensics Secur. 2009 Dec;4(4):790–801."
28 S. Sudharsanan, "Shared key encryption of JPEG color images," IEEE Trans. Consum. Electron., vol. 51, no. 4, pp. 1204–1211, Nov. 2005, https://doi.org/10.1109/TCE.2005.1561845.
29 Cimato S, De Prisco R, De Santis A. Contrast optimal colored visual cryptography schemes. In: 2003 IEEE Information Theory Workshop (ITW); 2003 Mar 31-Apr 5; Paris, France. IEEE; 2003. p. 139–42.
30 Chang C-C, Tsai C-S, Chen T-S. A new scheme for sharing secret color images in computer network. In: Proceedings of the Seventh International Conference on Parallel and Distributed Systems (ICPADS); 2000 Jul 4-7; Iwate, Japan. IEEE; 2000. p. 21–7.
31 Naor M, Shamir A. Visual cryptography. Advances in Cryptology, EUROCRYPT, Springer-Verlag, vol. 950, pp. 1-12, 1995.