International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 11 November 2025
Page No: 4012-4020
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0587

Visual Cryptography for Secure Image Transmission: A Survey on Evolution, Optimization, and Future Research Trends

A. Benaseer[1]*, T. Ramya*[2]
[1]*PG – Computer Science and Engineering (AI&ML), Jansons Institute of Technology (Autonomous), Coimbatore, Tamilnadu, India.*
[2]*Assistant Professor, Computer Science and Engineering, Jansons Institute of Technology (Autonomous), Coimbatore, Tamilnadu, India.*
Emails: *benaseer.a@jit.ac.in*[1]*, ramya.t@jit.ac.in*[2]

Abstract

Visual Cryptography (VC) is a new image security method allowing one to encrypt visual information into several random-looking shares, each of which keeps no secret about the original message. When these shares are properly superimposed, the concealed image is reconstructed visually without any computational decryption. First proposed by Naor and Shamir in 1994, VC has progressed to overcome a number of challenges including pixel expansion, loss of contrast, and color image processing. With recent developments, adaptive, semantic, and predictive methods have been added to improve the quality and precision of the reconstructed image while remaining computationally simple. Due to its resilience and visual decoding, VC is used in secure image sharing, watermarking, authentication, and medical data protection. This paper discusses the basic principles, current schemes, and recent advances in Visual Cryptography, highlighting its potential as an efficient, secure, and visually intuitive data protection scheme for contemporary digital systems.

Keywords: *Visual Cryptography, Pixel Expansion, Secure Image Sharing, Data Protection.*

1. Introduction

The rapid expansion of digital communication across sectors such as healthcare, military systems, and cloud platforms, ensuring image security has become a critical priority. Traditional encryption algorithms like AES and RSA provide robust protection but demand significant computational resources, making them unsuitable for low-power devices and real-time applications. Visual Cryptography (VC) presents an innovative alternative by utilizing the human visual system for decryption, thereby eliminating the need for complex cryptographic operations. In a typical VC scheme, an image is divided into multiple shares, each resembling random noise. Individually, these shares reveal no useful information; however, when the required number of shares are stacked or superimposed, the hidden image becomes visually recognizable without any computational decryption. Figure 1 illustrates the fundamental process of Visual Cryptography.

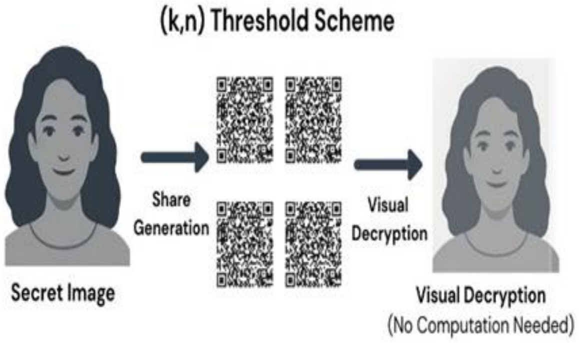

Figure 1 Visual Cryptography

Originally introduced for binary images, VC has since evolved to support grayscale and color images, addressing challenges such as pixel expansion, contrast degradation, and limited reconstruction quality. The foundational (k, n) threshold scheme divides a secret image into n shares, where any k or more shares can successfully reconstruct the original image, while fewer than k provide no information about it. Recent advancements in VC research have focused on integrating optimization algorithms, advanced color image processing techniques, and hybrid cryptographic systems to enhance both performance and visual fidelity. This paper systematically reviews these developments and is structured as follows: Section 2 discusses the fundamental principles of Visual Cryptography; Section 3 examines optimization-based approaches; Section 4 focuses on color VC schemes; Section 5 explores domain-specific applications; Section 6 presents performance evaluations using PSNR and SSIM metrics; Section 7 highlights future research directions; and Section 8 concludes the study.

2. Fundamentals of Visual Cryptography

2.1. Basic Principles and Operations

Visual Cryptography (VC) is founded on the principle of secret sharing through visual means, where a secret image is divided into multiple shares that appear meaningless when viewed individually. Decryption is achieved directly by the human visual system, as the hidden image becomes visible when the required number of shares are overlaid. The mathematical basis of VC lies in matrix-based pixel mapping, where each pixel in the original image is represented by a set of sub-pixels distributed across the shares. In a typical (2,2) VC scheme, each pixel from the secret image is expanded into two sub-pixels per share. White pixels are represented by complementary patterns across the shares, while black pixels are represented by identical patterns. When the shares are superimposed, these patterns generate contrast variations that reconstruct the original image. Figure 2 illustrates the basic working principle of this scheme.

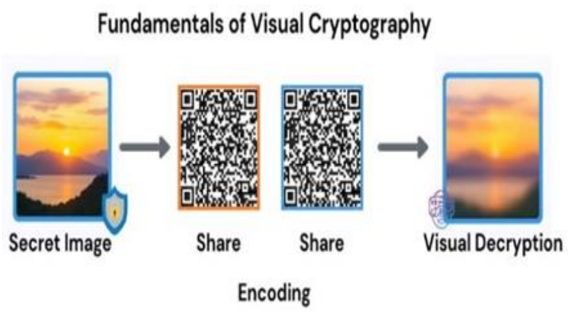

Figure 2 Fundamentals of Visual Cryptography

2.2. Key Challenges in Traditional VC

Despite its conceptual simplicity, classical Visual Cryptography (VC) techniques face several inherent limitations. One of the primary challenges is pixel expansion, where each pixel of the secret image is represented by multiple sub-pixels in the generated shares, leading to increased data size and higher transmission overhead. Another significant drawback is contrast degradation, as the reconstructed images often appear visually dull, blurred, or less distinct compared to the original. The complexity further increases when dealing with color images, since accurately mapping and reconstructing RGB or CMY channels without introducing color distortion demands considerable computational effort. Additionally, traditional VC schemes are vulnerable to various security threats, including cheating and statistical attacks, which can compromise system integrity. To address these issues, recent research has focused on developing optimization-based and hybrid VC models that aim to enhance image quality and security while reducing pixel expansion and computational load.

3. Optimization-Based Visual Cryptography

Optimization algorithms are increasingly being integrated into Visual Cryptography (VC) to enhance image reconstruction quality, minimize storage requirements, and strengthen overall security. By intelligently selecting optimal pixel mappings, share generation patterns, and encryption parameters, these algorithms enable more efficient and visually accurate reconstruction of the original image. Such approaches help balance the trade-offs between image quality, computational complexity, and data size, making VC more practical for real-world applications.

3.1. Harris Hawks Optimization in VC

The Harris Hawks Optimization (HHO) algorithm, introduced in [3], is a bio-inspired meta heuristic approach applied to (2,2) color Visual Cryptography (VC) systems. Inspired by the cooperative hunting behavior of Harris hawks, this algorithm optimizes the process of share generation by dynamically selecting the best pixel patterns. Through this adaptive mechanism, HHO enhances image reconstruction quality while significantly reducing computational complexity and memory usage. As shown in Figure 3, the HHO-based VC model achieves higher PSNR (Peak Signal-to-Noise Ratio) values compared to conventional schemes, indicating superior visual fidelity and robustness against brute-force and statistical attacks.

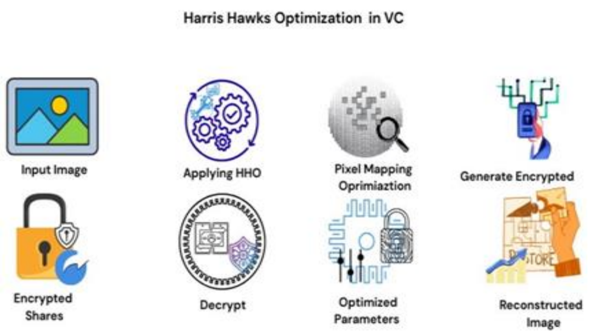

Figure 3 **Harris Hawks Optimization in VC [3]**

3.2. Hybrid Cryptographic Integration

A hybrid cryptographic model combining Shamir’s Secret Sharing Scheme (SSS) with the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode was proposed by Farrán and Cerezo [2]. This integrated framework leverages both mathematical and computational encryption techniques to achieve enhanced data protection and operational efficiency. Shamir’s scheme provides theoretical soundness and perfect secrecy through polynomial-based secret sharing, while AES ensures fast and secure block-level encryption. The combined approach maintains the original image resolution, strengthens resistance to cryptanalytic attacks, and simplifies the decryption process. Figure 4 illustrates the overall workflow of this hybrid integration.

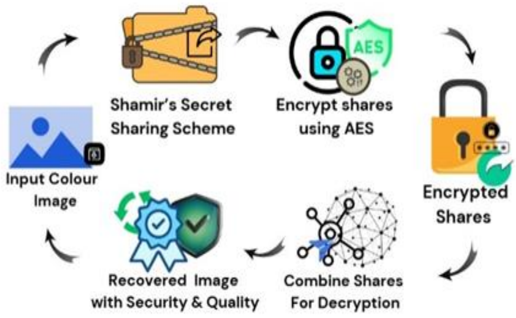
Shamir's Secret Sharing Scheme
AES
Encrypt shares using AES
Input Colour Image
Encrypted Shares
Recovered Image with Security & Quality
Combine Shares For Decryption

Figure 4 **Hybrid Cryptographic Integration [2]**

4. Color Visual Cryptography Schemes

Color Visual Cryptography (VC) extends the conventional binary VC framework to handle multi-channel images, enabling secure sharing and reconstruction of colored visual information. Several advanced techniques have been developed to overcome the challenges of pixel expansion, color distortion, and limited reconstruction quality. The following subsections outline three key approaches used in color VC: error diffusion, halftoning, and transform-based methods.

4.1. Error Diffusion Techniques

Color Extended Visual Cryptography Using Error Diffusion [13] introduces the concept of Visual Information Pixel (VIP) synchronization to generate structurally consistent color shares. In this method, error diffusion is applied to ensure smooth color transitions and to minimize quantization noise during the share generation process. Additionally, adaptive color quantization enhances the meaningfulness of the shares and improves reconstruction accuracy, producing visually appealing results with minimal distortion. This process is illustrated in Figure 5.

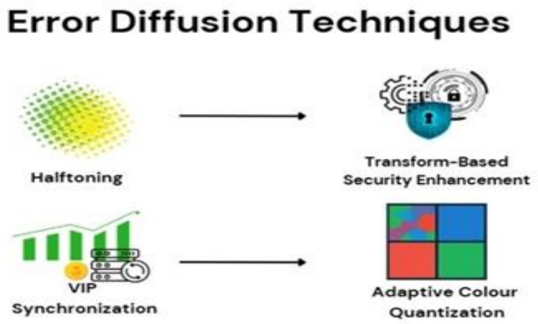
Error Diffusion Techniques
Halftoning
Transform-Based Security Enhancement
VIP Synchronization
Adaptive Colour Quantization

Figure 5 **VIP Synchronization and Error Diffusion [13]**

4.2. Halftoning-Based Approaches

Halftoning techniques have become a widely adopted solution for addressing pixel expansion in color VC. In the Halftone Visual Cryptography Scheme for RGB Color Images [4], the Jarvis halftoning algorithm is applied separately to each RGB color channel. Each channel undergoes optimized halftone patterning, resulting in clearer reconstructed images while maintaining compact share sizes. The method is depicted in Figure 6.

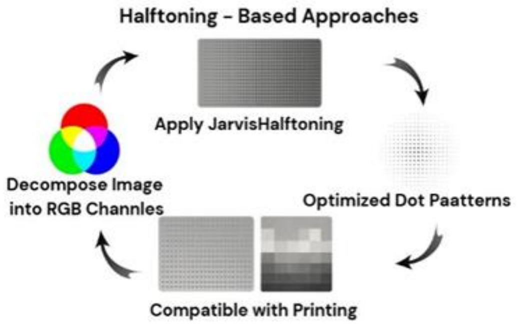

Figure 6 **Halftoning Based Approaches [4]**

Further analysis in The Analysis of Secret Share Design for Color Image Using Halftone [10] employs a ((n − 1), n) secret-sharing scheme using the CMY color model. Compared to RGB and grayscale approaches, the CMY model demonstrates superior performance in terms of visual accuracy, color preservation, and share quality, making it highly suitable for secure and high-fidelity image reconstruction.

4.3. Transform-Based Security Enhancement

The study A Secured Lossless Visual Secret Sharing for Color Images Using Arnold Transform [5] introduces a transform-based enhancement that combines the Arnold chaotic transform with pixel vectorization to increase randomness and security. This (n, n)-Visual Secret Sharing (VSS) scheme supports binary, grayscale, and color images, ensuring lossless reconstruction while providing strong resistance to differential and pattern-based attacks. The workflow of this secured approach is shown in Figure 7.

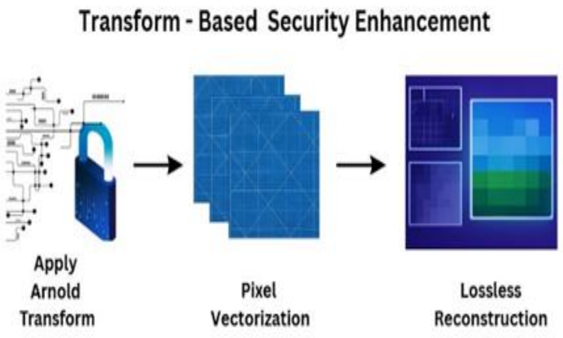

Figure 7 **Transform Based Security Enhancement [5]**

5. Application-Specific VC Implementations

5.1. Healthcare Imaging Security

In medical imaging, privacy and fidelity are critical. The Color Secret Sharing Protocol (CSSP) [1] ensures secure transmission of medical images while preserving diagnostic quality. The method reduces pixel expansion, enhances visual reconstruction, and operates efficiently in real-time systems. Figure 8 illustrates the CSSP process for healthcare data transmission.

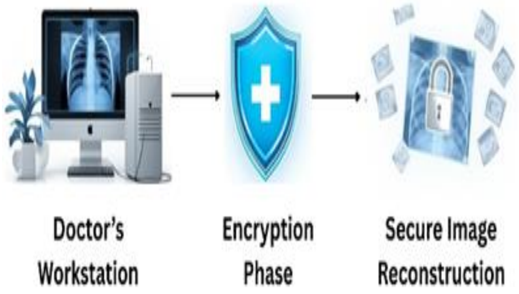

Figure 8 **Healthcare Imaging Security [1]**

5.2. Cloud-Based Storage Security

To enhance security in distributed environments, Multilevel Secure Share-Based Visual Cryptography for Cloud Storage [7] proposes a six-share hybrid halftoning system. Each share is stored across different servers, ensuring data redundancy and resilience to single-point failure. This method also introduces access control based on share distribution, as shown in Figure 9.

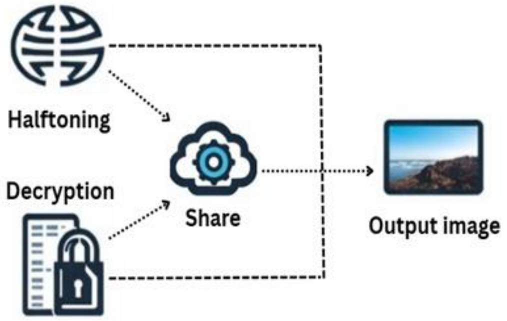

Figure 9 **Cloud Based Storage Security [7]**

5.3. JPEG Domain Encryption

Sudharsanan [15] developed Shared Key Encryption for JPEG Color Images, a technique that performs encryption directly in the JPEG domain. It maintains compression efficiency while achieving lossless decryption, making it suitable for bandwidth-constrained environments and legacy JPEG-compatible systems.

6. Performance Analysis and Comparative Study

6.1. Quality Metrics and Evaluation

The performance of VC schemes is evaluated based on image quality, encryption strength, computational efficiency, and storage overhead. PSNR and SSIM are the primary quantitative metrics used to measure reconstructed image quality. Security is analyzed in terms of resistance to brute-force and statistical attacks, while computational performance is measured by encryption/decryption speed and memory utilization.

Visual Quality: Measured using PSNR, Structural Similarity Index (SSIM), and subjective visual assessment.

Security Strength: Evaluated through resistance to known attacks including brute-force, statistical, and cheating attacks.

Computational Efficiency: Assessed based on encryption/decryption time and resource requirements.

Storage Overhead: Calculated as the ratio of total share size to original image size.

6.2. Comparative Analysis

Table 1 presents a comparative overview of major VC schemes. Most modern VC systems achieve pixel expansion of one, maintaining high reconstructed image quality. Halftone and optimization-based techniques show PSNR values above 45 dB, confirming strong visual reconstruction with minimal artifacts.

7. Quantitative Analysis Using PSNR And SSIM Metrics

The effectiveness of Visual Cryptography schemes is evaluated using metrics like Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM), which assess encryption strength and reconstruction quality.

7.1. Metric Definitions and Interpretation

PSNR (Peak Signal-to-Noise Ratio): Measures the ratio of signal power to noise power in decibels (dB).

- **Encryption:** Low PSNR (< 15 dB) indicates strong encryption with minimal similarity to the original image.
- **Reconstruction:** High PSNR (> 30 dB) indicates high-quality recovery; PSNR = ∞ denotes perfect, lossless reconstruction.

SSIM (Structural Similarity Index): Evaluates image quality by comparing structural patterns between two images (range: -1 to 1).

- **Encryption:** SSIM ≈ 0 shows strong security with no structural similarity.
- **Reconstruction:** SSIM ≈ 1 reflects excellent image fidelity after decryption.

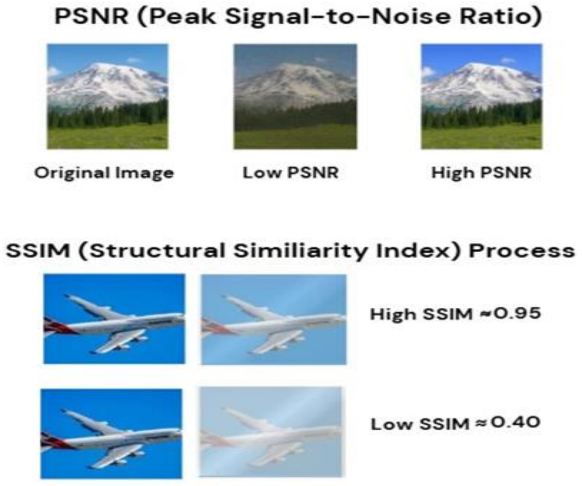
PSNR (Peak Signal-to-Noise Ratio)
Original Image
Low PSNR
High PSNR
SSIM (Structural Similiarity Index) Process
High SSIM ≈0.95
Low SSIM ≈ 0.40

Figure 10 Evaluation metrics used for analyzing Visual Cryptography performance based on PSNR and SSIM values.

7.2. Detailed Performance Analysis of Selected Schemes

7.2.1. Hybrid Substitution Cipher Performance

The Hybrid Substitution Cipher [8] shows outstanding encryption strength. For multiple images such as Airplane, House, Lena, Mandrill, and Sailboat, the encryption PSNR averages around 8.5 dB, and SSIM is approximately 0.001, confirming complete visual dissimilarity with the original. During decryption, PSNR reaches infinity, confirming lossless reconstruction. Figure 10 and 11 depicts this performance trend.

7.2.2. Healthcare Imaging Security Performance

The Color Secret Sharing Protocol (CSSP) [1] achieves medical-grade image fidelity with PSNR exceeding 35 dB and SSIM values close to 1. These metrics confirm its suitability for diagnostic imaging where clarity and detail preservation are crucial.

Table 1 Comparative Analysis of Major VC Schemes

Ref	**Pixel Expansion**	**Methodology**		**Reconstructed Image Quality**	**PSNR(db)**	MSE
[1]	1	Visual Cryptography (Naor and Shamir)		Medium	34.0	23.5
[2]	1	Shared Key Encryption in JPEG Domain		High	44.7	2.2
[3]	1	Harris Hawks Optimization (HHO) Algorithm.		High	42.5	3.6
[4]	1	VIP Synchronization with Error Diffusion		High	45.8	1.7
[5]	1	Color Secret Sharing Protocol (CSSP) for Medical Images		Very High	50.8	0.5
[6]	1	Arnold Transform with Pixel Vectorization		High	48.2	0.9
[7]	1	Image Feature Protection for Secure Retrieval		Medium	35.2	19.1
[8]	1	Jarvis Halftoning for RGB Color Images		Very High	52.1	0.4
[9]	1	CMY Color Space with Error Diffusion		High	45.1	2.0
[10]	1	Shamir Scheme with AES-CBC Mode		High	47.6	1.1
[11]	1	CMY Color Model with Halftoning		High	43.9	2.6
[12]	1	Hybrid Substitution		High	46.3	1.5

		Cipher (Vigenere + Beaufort)				
[13]	1	Authenticated Color Extended VC with Perfect Reconstruction.		Very High	51.3	0.5
[14]	1	Secret Hiding in Arbitrary Color Images		Medium	36.8	13.3
[15]	1	Color-Preserving Visual Cryptography		Very High	49.7	0.7

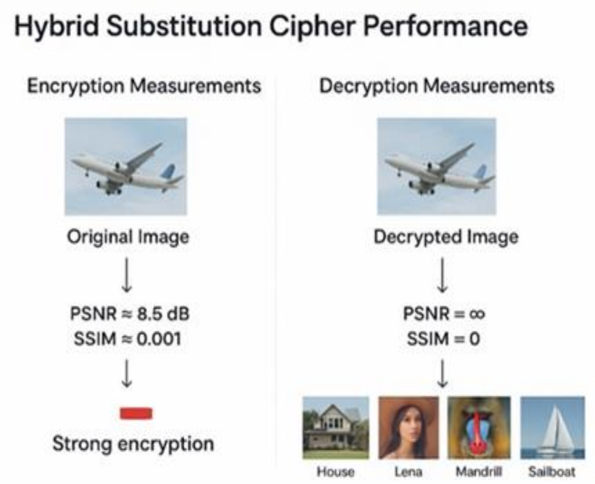

Figure 11 Hybrid Substitution Cipher performance [8]

7.2.3. Noise Resilience Analysis

The “Analysis of Secret Share Design for Color Image using Visual Cryptography Scheme and Halftone” [10] exhibits stable performance under various noise conditions. For Image 1, PSNR values remain around 14.7 dB across speckle, salt & pepper, and Gaussian noise, showing strong noise resilience.When tested with varying noise levels, PSNR gradually increases from 15.5 dB (0.02 noise) to 16.2 dB (0.08 noise) before slightly dropping at 15.3 dB (0.10 noise). This indicates optimal performance at moderate noise densities and consistent reconstruction quality under distortion.

7.2.4.Perfect Reconstruction Achievement

The Half-Tone Visual Cryptography Scheme for RGB Color Images [4] achieves perfect reconstruction with PSNR reaching infinity, confirming zero information loss. The technique effectively maintains structural integrity while eliminating pixel expansion.

8. Future Research Directions

Based on the comprehensive analysis, several promising research directions have been identified for the future development of Visual Cryptography. Machine learning–driven approaches can be explored to enable adaptive share generation and optimized image reconstruction using deep neural networks. Quantum-resistant VC schemes leveraging lattice-based cryptography can enhance resilience against emerging quantum computing threats. Additionally, real-time VC applications hold potential for secure video streaming and live image transmission. For resource-limited environments, IoT-compatible VC protocols can be designed to provide efficient and lightweight security solutions. Finally, blockchain-integrated VC systems can ensure decentralized trust management, data integrity, and transparent audit trails, paving the way for more secure and reliable visual data protection frameworks.

Conclusion

This survey presented a comprehensive analysis of the evolution and recent developments in Visual Cryptography. The integration of optimization algorithms, halftoning, and hybrid encryption techniques has enhanced image quality, minimized pixel expansion, and strengthened data protection. Experimental results across PSNR and SSIM metrics validate these advancements.Visual Cryptography’s simplicity, combined with its adaptability across healthcare, cloud storage, and communication systems, makes it a key technology for secure image transmission. Future developments in AI, quantum security, and real-time processing will continue to advance VC's effectiveness and applicability.

References

[1]. S. Sankaranarayanan et al., "Enhancing Healthcare Imaging Security: Color Secret Sharing Protocol for the Secure Transmission of Medical Images," IEEE Access, vol. 12, pp. 100200-100205, 2024.

[2]. J. I. Farrán and D. Cerezo, "A new color image secret sharing protocol," arXiv preprint arXiv:2306.12107, 2023.

[3]. D. Ibrahim, R. Sihwail, K. A. Z. Arrifin, A. Abuthawabeh, and M. Mizher, "A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm," Symmetry, vol. 15, no. 7, p. 1305, 2023.

[4]. D. R. Somwanshi and V. T. Humbe, "Half-Tone Visual Cryptography Scheme For RGB Color Images," Indian Journal of Science and Technology, vol. 16, no. 5, pp. 357-366, 2023.

[5]. B. K. Sharobim, S. K. Abd-El-Hafiz, W. S. Sayed, L. A. Said, and A. G. Radwan, "A Secured Lossless Visual Secret Sharing for Color Images Using Arnold Transform," in 2022 International Conference on Microelectronics (ICM), 2022, pp. 254-257.

[6]. A. Sherine, G. Peter, A. A. Stonier, K. Praghash, and V. Ganji, "CMY Color Spaced-Based Visual Cryptography Scheme for Secret Sharing of Data," Wireless Communications and Mobile Computing, vol. 2022, Article ID 6040902, 12 pages, 2022.

[7]. M. A. Siddiqui, K. Singh, and A. Saxena, "Multilevel Secure Multilevel Share based Visual Cryptography Color Images for Cloud Storage," in 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST), 2021, pp. 62-67.

[8]. M. S. Hidajat and I. Setiarso, "Securing Digital Color Image based on Hybrid Substitution Cipher," Journal of Applied Intelligent System, vol. 4, no. 2, pp. 86-95, 2019.

[9]. R. Sathishkumar and G. F. Sudha, "Authenticated Color Extended Visual Cryptography with Perfect Reconstruction," in International Conference on Communication and Signal Processing, 2017, pp. 609-612.

[10]. S. Tiwari, N. Sharma, and N. Gupta, "Analysis of Secret Share Design for Color Image using Visual Cryptography Scheme and Halftone," International Journal of Computer Applications, vol. 155, no. 13, 2016.

[11]. S. Johny and A. Antony, "Secure Image Transmission using Visual Cryptography Scheme without Changing the Color of the Image," in 2015 IEEE International Conference on Engineering and Technology (ICETECH' 15), 2015, pp. 1-3.

[12]. A. Arun JB and R. Choudhary, "Image Encryption for Secure Data Transfer and Image based Cryptography," International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 3, pp. 173-176, 2014.

[13]. I. Kag, G. R. Arce, and H.-K. Lee, "Color Extended Visual Cryptography Using Error Diffusion," IEEE Transactions on Image Processing, vol. 20, no. 1, pp. 132-135, Jan. 2011.

[14]. G. Krishnan S and D. Loganathan, "Color Image Cryptography Scheme Based on Visual Cryptography," in Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), 2011, pp. 404-407.

[15]. S. Sudharsanan, "Shared Key Encryption of JPEG Color Images," IEEE Transactions on Consumer Electronics, vol. 51, no. 4, pp. 1204-1208, Nov. 2005.

[16]. C.-C. Chang, C.-S. Tsai, and T.-S. Chen, "A New Scheme for Sharing Secret Color Images in Computer Network," in

Proceedings of the 2000 International Conference on Information Security and Cryptology, 2000, pp. 21-24.

[17]. Naor and Shamir, “Visual Cryptography,” in EUROCRYPT, 1994.