International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

Efficient Cognitive Visual Cryptography for Secure Image Transmission

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

Abstract
Visual Cryptography (VC) is a technique used to protect images by dividing them into multiple meaningless shares, where the original image becomes visible only when the correct shares are combined. Traditional Cognitive Visual Cryptography (CVC) approaches mainly depend on stacking these shares for reconstruction, but they often result in larger image sizes, reduced visual quality, and limited practical usability. To overcome these challenges, this work introduces an enhanced CVC framework that makes effective use of human visual perception during the reconstruction process. Instead of relying on complex computations, the human eye itself plays a key role in interpreting the hidden image, making the recovery process simple and intuitive. The proposed method applies adaptive encoding and decoding based on image characteristics such as contrast and complexity, ensuring that important visual details are preserved. Perceptual modelling further improves robustness against noise and lighting variations. As a result, the reconstructed images exhibit better clarity and reliability. In addition, shifting much of the decoding responsibility to human perception reduces computational effort and energy consumption. The proposed approach therefore offers a practical and user-friendly solution for secure image sharing, with potential applications in areas such as real-time authentication and secure digital document transmission.

Keywords: *Cognitive Visual Cryptography, Visual Cryptography, Human Visual Perception, Secure Image Sharing, Image Security*

1. Introduction
In the present digital era, digital images play a vital role in information representation and communication. Images are widely used in sensitive and critical applications such as medical diagnosis, biometric authentication, military surveillance, e-governance systems, cloud storage, and multimedia communication. With the rapid growth of the internet and wireless networks, image transmission over open and insecure channels has increased significantly, making image data highly vulnerable to threats like unauthorized access, interception, manipulation, and misuse. Securing digital images is more challenging than securing textual data because images have large data size, high redundancy, and strong correlation between neighboring pixels. Traditional cryptographic algorithms such as AES, DES, and RSA provide strong security but are not always suitable for image data. These methods involve complex computations, high processing time, and strict key management, which reduce efficiency, especially in real-time and resource-constrained applications. To overcome these limitations, Visual Cryptography was introduced as an alternative image security technique. In Visual Cryptography, a secret image is divided into multiple shares, each appearing as random noise and revealing no information individually. The original image can be reconstructed simply by stacking the required shares together, without using any mathematical computation or secret key. However, traditional Visual Cryptography suffers from drawbacks such as pixel expansion, reduced contrast, poor visual quality, and increased storage requirements. Additionally, the reconstructed images often appear noisy and lack perceptual clarity, making them difficult for human interpretation. These limitations restrict the practical applicability of

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

traditional Visual Cryptography in real-time and high-quality image security systems. To address these issues, Cognitive Visual Cryptography has been proposed as an advanced approach. **Figure 1** shows the basic concept of Visual Cryptography. The secret image is divided into two meaningless noise-like shares, namely Share 1 and Share 2. Individually the shares reveal no information, but when both shares are combined, the original image is visually reconstructed without any computation.

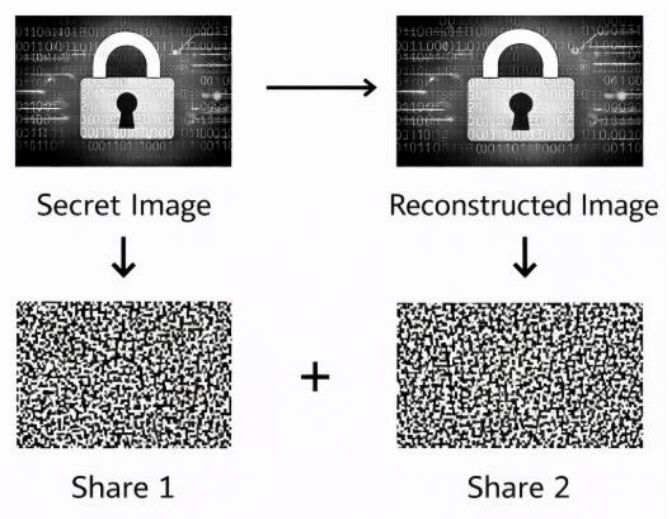

Figure 1 Visual Cryptography – Secret Image Sharing and Reconstruction

2. Fundamentals of Visual Cryptography

2.1. Basic Concept of Visual Cryptography

Visual Cryptography encodes each pixel of a secret image into multiple sub-pixels that are distributed across different shares. Each share alone appears meaningless, but when stacked together, the sub-pixels combine to form the original image.

2.2. (k, n) Threshold Scheme

In a (k, n) threshold Visual Cryptography scheme, the secret image is divided into n shares, and at least k shares are required to reconstruct the image. Any number of shares less than k reveals no information about the original image. **Figure 2** illustrates the (k, n) Visual Cryptography scheme. The secret image is split into multiple shares, where fewer than k shares reveal no information about the secret image. When at least k valid shares are combined, the secret image is successfully revealed. This scheme provides flexibility, fault tolerance, and strong access control.

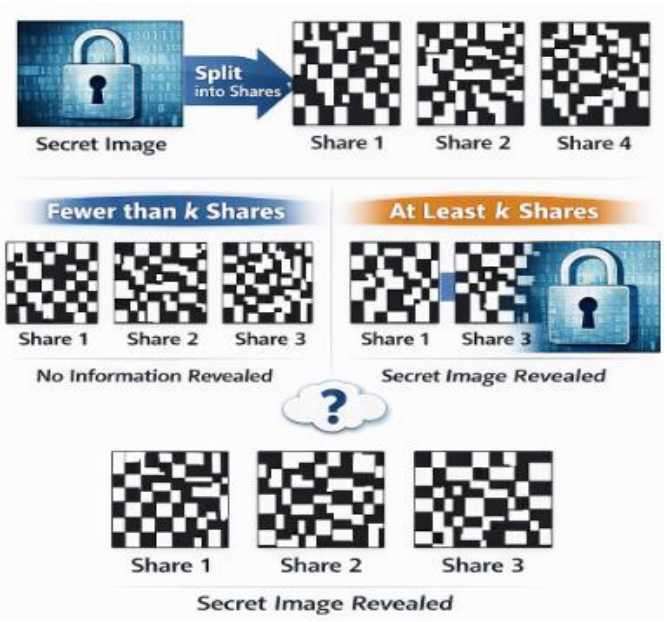

Figure 2 (k, n) Threshold Visual Cryptography Scheme

2.3. (2,2) Visual Cryptography Scheme

In the (2,2) scheme, the secret image is split into exactly two shares. Both shares are mandatory for reconstruction. This is the simplest and most widely used Visual Cryptography model due to its simplicity and strong security.

2.4. Pixel Expansion

Pixel expansion refers to the increase in the number of pixels in the shares compared to the original image. Although pixel expansion improves security, it increases storage requirements and reduces image resolution, which affects visual quality.

2.5. Contrast and Visual Quality

Contrast plays a crucial role in the visibility of reconstructed images. Low contrast makes it difficult for the human eye to recognize patterns and details. Improving contrast is essential for practical usability of Visual Cryptography systems.

2.6. Security Properties of Visual Cryptography

Visual Cryptography provides:

- Perfect secrecy for individual shares
- No information leakage from a single share

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

- Resistance to brute-force and statistical attacks
- Keyless decryption using human visual perception

3. Literature Review

Visual Cryptography (VC) was first introduced by Naor and Shamir [17], where a secret image is divided into multiple shares such that only an authorized subset of shares can visually reconstruct the original image. This foundational work established threshold-based secret sharing schemes that provided strong access control without computational decryption. Later research extended this concept to color images to improve practical applicability. Chang et al. [16] and Kang et al. [13] proposed color visual cryptography schemes using color decomposition and error diffusion techniques, enabling secure color image sharing but at the cost of increased pixel expansion and reduced visual quality. To address color handling and reconstruction accuracy, several researchers explored RGB and CMY color space–based approaches. Somwanshi and Humbe [4] introduced a halftone-based visual cryptography scheme for RGB images, which improved perceptual appearance but suffered from low contrast. Sherine et al. [6] proposed a CMY color space–based scheme to enhance color preservation, though complexity increased with additional processing stages. Optimization-based methods, such as the Harris Hawks Optimization–based approach by Ibrahim et al. [3], aimed to enhance security and reconstruction quality but introduced higher computational overhead. Recent studies have focused on application-driven security. Sankaranarayanan et al. [1] proposed a color secret sharing protocol for secure medical image transmission, emphasizing confidentiality in healthcare systems. Farrán and Cerezo [2] developed a new color image secret sharing protocol to reduce information leakage and improve reconstruction accuracy. Hybrid approaches combining traditional cryptography with visual cryptography were also explored to strengthen security [8], [12], but these methods reintroduced challenges such as key management, increased processing time, and dependency on decryption algorithms. Despite these advancements, most existing visual cryptography schemes still suffer from limitations such as high pixel expansion, poor contrast, color distortion, and lack of perceptual optimization [9], [10], [11]. These drawbacks reduce usability in real-time and human-centric applications. To overcome these issues, Cognitive Visual Cryptography has emerged as an improved paradigm that integrates human visual perception and cognitive principles to enhance visual clarity, reduce pixel expansion, and provide a more practical and visually efficient solution for secure image communication.

4. Limitations of Existing System

- **Pixel Expansion Problem:** Traditional VC systems significantly increase image size, leading to higher memory and bandwidth requirements.
- **Contrast Degradation:** Reconstructed images often have poor contrast, making fine details difficult to interpret.
- **Color Image Processing Issues:** Independent processing of RGB channels increases computational complexity and may cause color distortion.
- **Storage and Transmission Overhead:** Multiple large shares increase storage cost and transmission time.
- **Security Vulnerabilities:** Lack of authentication may allow fake or tampered shares to be introduced.

5. Cognitive Visual Cryptography

Cognitive Visual Cryptography (CVC) is an advanced form of traditional Visual Cryptography that enhances image security by incorporating principles of human cognition and visual perception into the encryption and reconstruction process [5]. Unlike conventional approaches that rely solely on pixel-level manipulation, CVC focuses on how humans perceive visual information such as contrast, structure, and patterns. By integrating these perceptual aspects, Cognitive Visual Cryptography aims to overcome the limitations of traditional Visual Cryptography, particularly poor visual quality and high pixel expansion, while maintaining strong security without complex decryption mechanisms.

5.1. Role of Human Visual System (HVS)

The Human Visual System (HVS) plays a crucial role in Cognitive Visual Cryptography, as it is inherently

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

more sensitive to edges, contrast variations, and structural similarity than to exact pixel values [7]. CVC exploits these characteristics by optimizing share generation and reconstruction based on perceptual importance rather than precise numerical accuracy. **Figure 3** shows the working framework of Cognitive Visual Cryptography (CVC). It integrates human cognition and visual perception in the cryptographic process to enhance security and improve the visual quality of the reconstructed image. As a result, even when minor pixel-level distortions exist, the reconstructed image remains visually clear and recognizable to the human eye. This perceptual advantage allows Cognitive Visual Cryptography to improve image clarity and usability without compromising security.

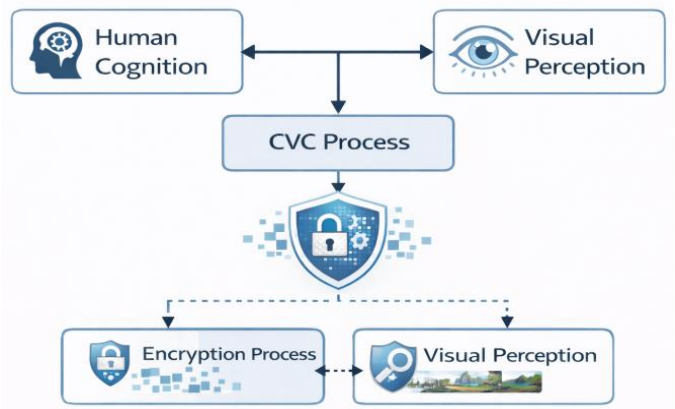

Figure 3 Cognitive Visual Cryptography (CVC) Framework

5.2. Difference between Visual Cryptography and Cognitive Visual Cryptography

Traditional Visual Cryptography primarily focuses on pixel-level security, where image protection is achieved by expanding pixels into sub-pixels and distributing them across multiple shares. While this approach ensures strong secrecy, it often results in poor contrast and reduced visual quality. In contrast, Cognitive Visual Cryptography emphasizes perceptual clarity and human interpretability by incorporating cognitive and visual perception models. CVC prioritizes how the reconstructed image appears to the human observer, leading to better contrast, reduced pixel expansion, and improved overall visual quality.

5.3. Advantages of Cognitive Visual Cryptography

Cognitive Visual Cryptography offers several significant advantages over traditional Visual Cryptography techniques. It reduces pixel expansion, thereby lowering storage and transmission overhead. The incorporation of human perceptual principles improves contrast and visual clarity in reconstructed images, making them easier to interpret [14]. CVC does not require any mathematical decryption or secret key, as reconstruction is performed visually using the human eye. Furthermore, its human-centric security approach makes it highly suitable for real-world applications where both security and visual quality are equally important.

6. Proposed System

6.1. System Overview

The proposed system is based on Cognitive Visual Cryptography, which aims to enhance image security by generating perceptually optimized cryptographic shares [15]. The main objective of the system is to provide strong confidentiality, reduced pixel expansion, and improved visual clarity while ensuring that individual shares do not reveal any meaningful information. **Figure 4** illustrates the pattern-based Visual Cryptography process. Two random noise patterns (Pattern 1 and Pattern 2) are individually meaningless, but when they are combined, the human visual system perceives the hidden secret image. The system is designed to be simple, secure, and suitable for real-world image communication applications.

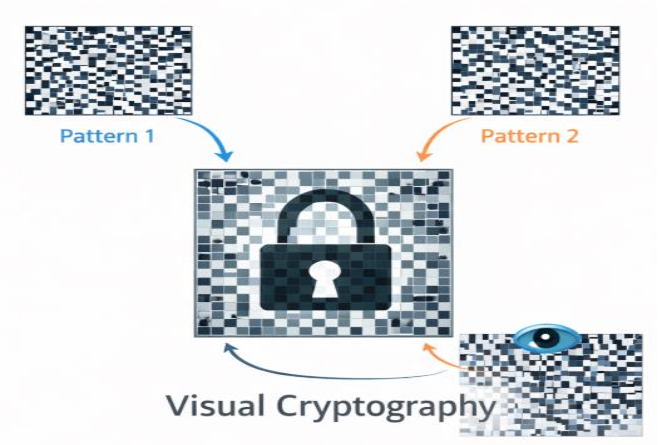

Figure 4 Pattern Overlay Mechanism in Visual Cryptography

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

6.2. System Workflow

The overall workflow of the proposed system follows a sequential process. Initially, the input image is provided to the system and undergoes preprocessing. The image is then encrypted and divided into multiple secure shares during the share generation phase. These shares are transmitted independently over separate communication channels to enhance security. At the receiver side, the required shares are combined, and the original image is visually reconstructed using the human visual system without the need for computational decryption.

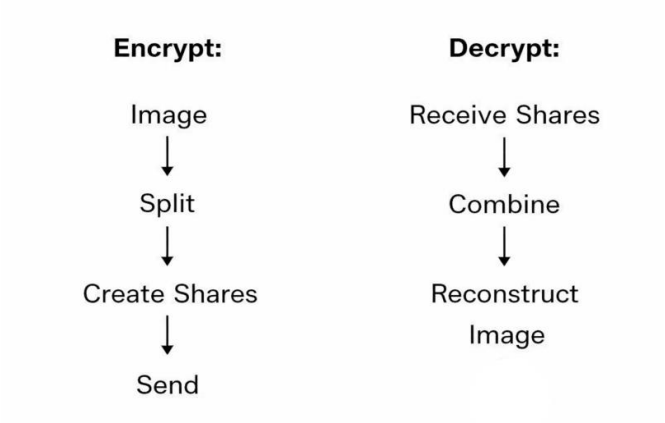

Figure 5 Encryption and Decryption Process in Visual Cryptography

6.3. Encryption Phase

During the encryption phase, the input image is first preprocessed to remove noise and normalize pixel values. For color images, the image is divided into Red, Green, and Blue (RGB) channels, which are processed independently. Random matrices are generated and combined with the image pixel values to introduce randomness and unpredictability. This process ensures that the encrypted shares appear meaningless and do not expose any visual information related to the original image (**Figure 5**).

6.4. Share Generation Process

In the share generation process, the encrypted image data is converted into multiple shares. Each share either appears as random noise or as a visually meaningful cover image, depending on the design of the scheme. Individually, these shares do not reveal any information about the original image. Only when the required number of shares are combined does the hidden image become visible, ensuring strong security against unauthorized access.

6.5. Secure Transmission

Once the shares are generated, they are transmitted independently through separate communication channels. This independent transmission strategy significantly reduces the risk of interception and unauthorized reconstruction. Even if an attacker gains access to one or more shares, the original image cannot be recovered without all the required shares, thereby ensuring secure image communication.

6.6. Decryption and Reconstruction

Decryption and reconstruction are performed by visually stacking the received shares. Unlike conventional cryptographic systems, no secret key or mathematical decryption algorithm is required. The human visual system performs the decoding process by perceiving the combined shares and reconstructing the original image. Due to the perceptual optimization used during encryption, the reconstructed image exhibits improved contrast, clarity, and structural integrity.

7. System Architecture and Design

The system architecture consists of multiple layers including Presentation Layer, Application Layer, Processing Layer, Data Management Layer, and Network Layer. This layered design improves modularity, scalability, and security for efficient system performance. **Figure 6** represents the layered architecture of the Visual Cryptography system. It shows the flow from the presentation layer to the network and transmission layer, ensuring structured processing, secure data handling, and efficient image sharing.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

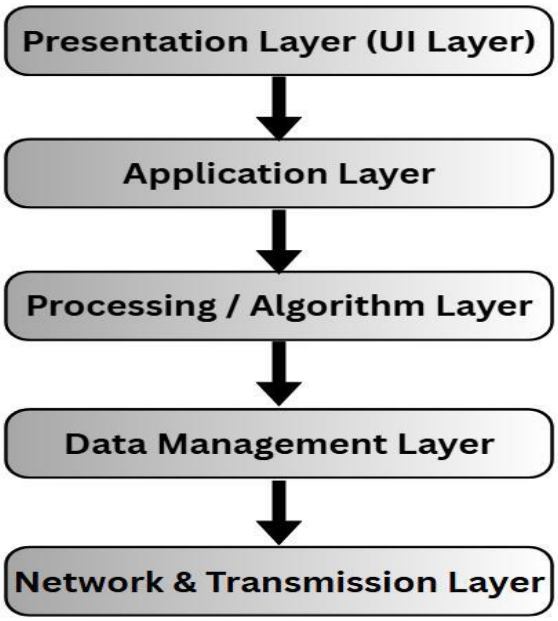

Figure 6 Layered System Architecture

8. Mathematical Model

8.1. Notations

In the proposed Cognitive Visual Cryptography system, mathematical notations are used to formally represent the image encryption and reconstruction process. Let $I(x,y)$denote the pixel intensity value of the original input image at spatial location (x, y). Let $R(x,y)$represent a randomly generated matrix of the same dimensions as the input image, which is used to introduce randomness and ensure security during share generation. All pixel operations are performed within the valid grayscale or color intensity range of 0 to 255.

8.2. Share Generation

Share generation is the encryption phase of the system, where the original image is converted into multiple secure shares. The first share $S_1(x,y)$is generated by adding the original image pixel value $I(x,y)$with the corresponding random matrix value $R(x,y)$and applying a modulo 256 operation to keep the pixel values within the valid range. The second share $S_2(x,y)$ consists solely of the random matrix values. These equations ensure that each share individually appears as random noise and does not reveal any information about the original image.

$$S_1(x,y) = (I(x,y) + R(x,y)) mod 256$$
$$S_2(x,y) = R(x,y)$$

8.3. Reconstruction

Reconstruction is the decryption phase, where the original image is recovered by combining the generated shares. The reconstructed image pixel $I'(x,y)$is obtained by subtracting the second share $S_2(x,y)$from the first share $S_1(x,y)$and applying a modulo 256 operation. This process effectively cancels out the random component and restores the original pixel values. Reconstruction does not require any cryptographic key or complex computation and relies only on the availability of the required shares.

$$I'(x,y) = (S_1(x,y) - S_2(x,y)) mod 256$$

9. Color Visual Cryptography

The RGB color model plays a crucial role in color visual cryptography by representing a color image as a combination of Red, Green, and Blue components. In the proposed system, the original color image is first decomposed into its individual RGB channels, and each channel is processed separately to generate secure cryptographic shares. This channel-wise processing helps in preserving color information while ensuring that no single share reveals meaningful visual content. By handling each color component independently, the system provides better control over encryption strength and reconstruction accuracy for color images. Additionally, transform-based approaches, such as frequency-domain processing, help in preserving important structural information like edges and textures while reducing noise and distortion. Together, these techniques significantly improve contrast, color fidelity, and visual clarity in the reconstructed image, making the Cognitive Visual Cryptography system more effective and visually reliable.

10. Implementation

The proposed system is implemented using **MATLAB** along with the **Image Processing Toolbox**, which provides a powerful and flexible environment for developing and testing visual cryptography algorithms. MATLAB's built-in functions for image manipulation, matrix operations, and visualization simplify the implementation of complex processes such as image decomposition, pixel-level operations, and channel-wise processing. The system is designed to support both **grayscale and color images**, allowing it to handle a wide range of input data. For color images, the RGB components

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

are processed independently, while grayscale images are handled as single-channel inputs, ensuring consistent encryption and decryption behavior across different image types. The system includes key functionalities such as **share generation**, **image reconstruction**, and **performance evaluation**. During share generation, secure cryptographic shares are created in such a way that no individual share reveals meaningful visual information. In **Figure 7** Reconstruction is performed by stacking or combining the required shares to recover the original image with minimal loss of visual quality. To assess system effectiveness, performance evaluation metrics such as contrast, visual quality, and reconstruction accuracy are analyzed using MATLAB's visualization and analysis tools. This comprehensive implementation framework ensures that the system is reliable, efficient, and suitable for experimental analysis and academic research in visual cryptography.

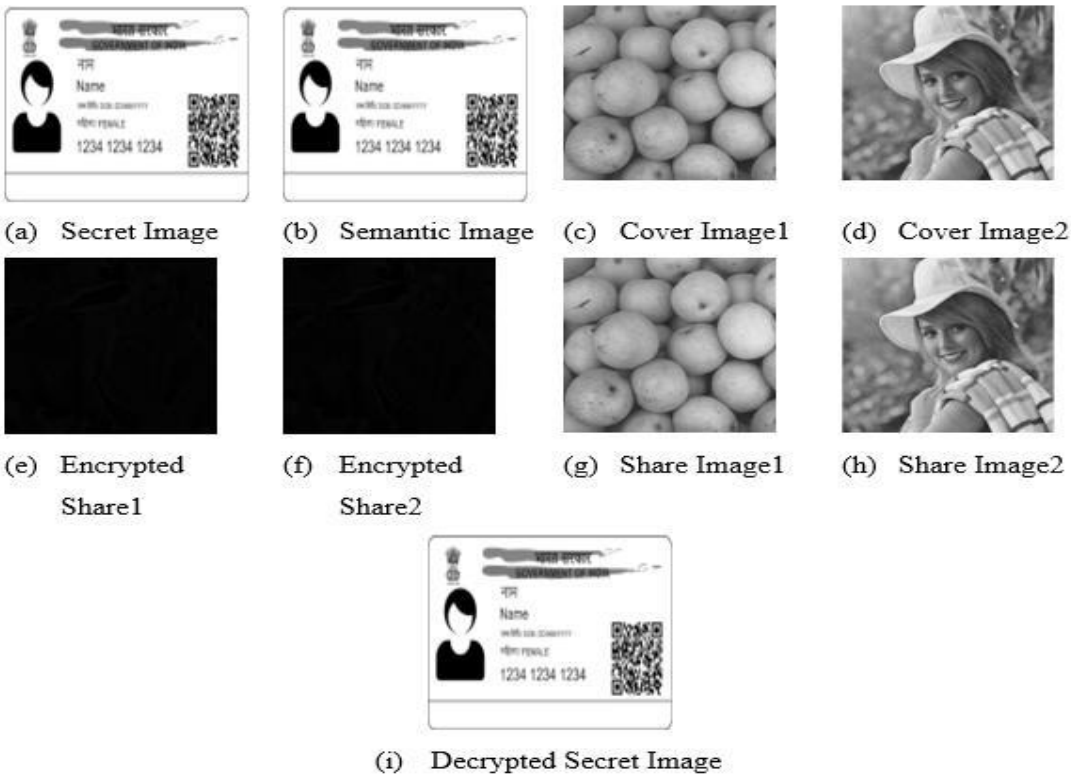

Figure 7 Experimental Results

11. Performance Analysis

Table 1 shows the Performance Evaluation of the Proposed Image Reconstruction and Visual Cryptography Scheme.

Table 1 Performance Evaluation of the Proposed Image Reconstruction and Visual Cryptography Scheme

Parameter	Observed Value	Performance
PSN R	Greater than 40 dB	High
PSNR Stability	Consistent across different test images	High

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

Noise Reduction	Very low noise in reconstructed images	High
SSIM	Greater than 0.90	High
Structural Preservation	Edges and textures well preserved	High
Contrast Quality	Improved contrast in reconstructed images	High
MSE	Very low error values	High
Pixel Accuracy	Minimal pixel-wise distortion	High
Reconstruction Quality	Clear and visually accurate output	High
Pixel Expansion	Reduced compared to traditional VC	Medium
Storage Requirement	Lower than existing VC schemes	Medium

12. Applications

- **Medical Image Security:** Used to protect sensitive medical images by dividing them into secure shares, allowing authorized reconstruction with clear visual.
- **Secure Document Sharing:** Ensures safe sharing of document images by encrypting them into multiple shares, avoiding unauthorized access and tampering.
- **Military Communication:** Protects sensitive military images by eliminating key-based decryption and preventing information leakage from individual shares.

13. Advantages

- **High Security:** Each share individually reveals no information about the original image, ensuring strong protection.
- **Improved Visual Quality:** Human visual perception is used to achieve better contrast and clearer reconstructed images.
- **Reduced Pixel Expansion:** Produces fewer extra pixels compared to traditional visual cryptography, improving efficiency.
- **Resistance to Attacks:** Random-noise–like shares protect against statistical and brute-force attacks.

14. Future Scope

The system can be extended to **video cryptography** for secure real-time communication, enhanced using **AI** to improve visual quality, integrated with **blockchain** for secure share management and tamper-proof logging, and adapted for **IoT environments** to enable efficient and low-computation secure image transmission.

Conclusion

The Cognitive Visual Cryptography system presented in this project successfully enhances the security of digital images by combining traditional visual cryptographic principles with human visual perception. Unlike conventional image encryption techniques that rely on complex mathematical computations and key management, the proposed approach utilizes the cognitive capabilities of the human visual system to perform decryption through visual stacking of shares. This keyless decryption mechanism simplifies the reconstruction process while maintaining a high level of security, as individual shares do not reveal any meaningful information about the original image. By incorporating perceptual optimization techniques, the proposed method reduces pixel expansion and significantly improves contrast, clarity, and structural preservation in the reconstructed images. Performance evaluation using standard image quality metrics such as PSNR, SSIM, and MSE demonstrates that the system achieves high reconstruction accuracy with minimal distortion. As a result, the Cognitive

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

Visual Cryptography system provides strong confidentiality, improved usability, and practical applicability, making it well suited for real-world applications such as medical image security, biometric authentication, secure document sharing, military communication, and cloud-based image storage.

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. Kang, 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

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 02 February 2026
Page No: 436-445
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0059

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.