International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Study of Visual Cryptography Techniques for Secure Distribution of Images Over the Internet

Mr Pranav Prakash Joshi[1], *Dr. Pravin Balajirao Tamsekar[2]*

[3]Research Scholar, School of Computational Sciences, SRTM University, Nanded
Email: ppj.ssbesitm@gmail.com
[2]Assitant Professor, Yeshwant Mahavidyalaya, Nanded

Abstract

With the rapid growth of Internet-based multimedia applications, secure image transmission has become a critical concern. Conventional cryptographic techniques rely on complex mathematical operations and key management mechanisms, which may not be suitable for lightweight or human-centric security systems. Visual Cryptography (VC) is a secret-sharing technique that allows images to be encrypted into multiple shares so that no single share reveals any information about the original image. Reconstruction is achieved by stacking the shares without requiring any computation. This paper presents a comprehensive study of visual cryptography techniques, including basic schemes, colour visual cryptography, security analysis, implementation challenges, and real-world case studies. The study highlights the effectiveness of VC in secure image distribution over the Internet and discusses its future research directions.

Keywords: Visual Cryptography, Image Security, Visual Secret Sharing, Secure Image Distribution, Internet Security.

I. INTRODUCTION

The Internet has revolutionised the way digital images are stored, shared, and transmitted. However, this openness also exposes sensitive image data to threats such as unauthorised access, interception, and tampering. Traditional encryption techniques such as AES and RSA provide strong security but require decryption keys and computational resources, making them unsuitable for certain applications, such as biometric authentication, cloud sharing, and low-power devices.

Visual Cryptography (VC), introduced by Naor and Shamir in 1994, provides a simple yet effective solution for secure image distribution. It encrypts an image into multiple shares, where each share individually appears as random noise. Only when a predefined number of shares are combined does the original image become visible to the human eye.

This paper aims to study various visual cryptography techniques and analyze their suitability for secure image distribution over the Internet.

II. LITERATURE REVIEW

Naor and Shamir first proposed the concept of visual cryptography using a (2,2) threshold scheme, where two shares are required to reveal the secret image [1]. Later, Verheul and van Tilborg extended this approach to general *(k, n)* schemes [2]. Research further evolved to include grayscale and colour visual cryptography to support real-world image data [3].

Recent studies focus on improving contrast, reducing pixel expansion, and generating meaningful shares for better usability. Visual cryptography has also been combined with watermarking, authentication, and cloud security frameworks [4].

III. VISUAL CRYPTOGRAPHY PRINCIPLES

A. Basic (2,2) Visual Cryptography Scheme

In a (2,2) scheme:

- The original image is converted into a binary image.
- Each pixel is expanded into multiple sub-pixels.
- Two shares are generated such that:
  1. Individually, shares reveal no information.
  2. When stacked, the secret image appears.

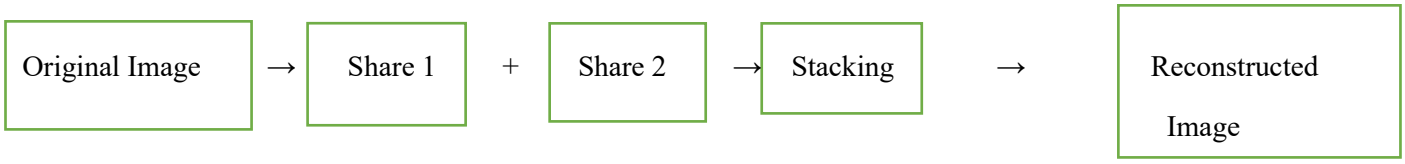

Fig. 1. Visual cryptography shares the generation and reconstruction processes.

B. (k, n) Threshold Visual Cryptography

In a (k, n) scheme:

- The secret image is divided into n shares.
- Any k shares can reconstruct the image.
- Fewer than k shares reveal no information.

This provides flexibility and fault tolerance in distributed systems.

C. Colour Visual Cryptography

Colour visual cryptography extends binary VC to RGB images:

- The image is decomposed into Red, Green, and Blue channels.
- Each channel undergoes visual cryptography separately.
- Channels are recombined during reconstruction.

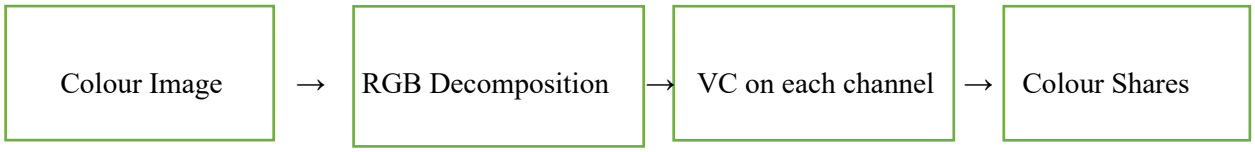

Fig. 2. Colour visual cryptography architecture.

IV. SECURITY ANALYSIS

Visual cryptography provides information-theoretic security. A single share contains random pixel distributions, making it impossible to infer the original image.

Technique	Key Required	Computation	Share Alone Reveals Info
AES	Yes	High	No
RSA	Yes	Very High	No
Visual Cryptography	No	None	No

Table I. Security feature comparison of cryptographic techniques.

V. IMPLEMENTATION FOR INTERNET IMAGE DISTRIBUTION

A. Share Transmission

Shares can be transmitted over different communication channels (email, cloud, messaging apps). Even if intercepted, attackers cannot reconstruct the image without all the required shares.

B. Storage in Cloud Systems

Shares can be stored on different cloud servers, reducing the risk of data leakage from a single breach.

C. Reconstruction

Reconstruction can be:

- Physical (printing and stacking)
- Digital (software overlay using XOR/OR operations)

VI. CASE STUDIES

Case Study 1: Secure Medical Image Sharing

Medical images such as MRI scans are highly sensitive. Using visual cryptography:

- The image is split into two shares.
- One share is stored in the hospital database.
- The second share is given to the patient.
- Only when both are combined can the image be viewed.

Benefit: Ensures patient privacy and prevents unauthorised access.

Case Study 2: Biometric Authentication Systems

Fingerprint images can be protected using VC:

- One share is stored in a server.
- One share is stored on a smart card.
- Authentication occurs only when both shares match.

Benefit: Eliminates the risk of biometric database leakage.

Case Study 3: Secure Cloud Image Storage

In cloud platforms:

- Image shares are stored across multiple cloud providers.
- No single provider has access to the complete image.

Benefit: Increased trust and reduced insider threats.

VII. ADVANTAGES AND LIMITATIONS

Advantages

1. No key management required
2. Simple decryption using human vision
3. High resistance to cryptographic attacks

Limitations

1. Pixel expansion increases storage size
2. Lower contrast in reconstructed images
3. Limited support for high-quality colour images

VIII. FUTURE SCOPE

Future research directions include:

- Reducing pixel expansion
- Visual cryptography for video streams
- Integration with blockchain for share verification
- AI-assisted visual cryptography optimization

IX. CONCLUSION

Visual cryptography is a powerful technique for secure image distribution over the Internet. By eliminating complex decryption and key management, it provides a human-centric security solution suitable for modern applications such as cloud computing, healthcare, and biometric systems. Although challenges such as image quality and storage overhead exist, ongoing research continues to enhance the practicality and efficiency of visual cryptography schemes.

REFERENCES

[1] M. Naor and A. Shamir, “Visual Cryptography,” *Advances in Cryptology—EUROCRYPT ’94*, Springer, pp. 1–12, 1994.

[2] E. R. Verheul and H. C. A. van Tilborg, “Constructions and Properties of k out of n Visual Secret Sharing Schemes,” *Designs, Codes and Cryptography*, vol. 11, no. 2, pp. 179–196, 1997.

[3] D. Shyu, “Image Encryption by Visual Cryptography,” *Pattern Recognition*, vol. 38, no. 6, pp. 959–972, 2005.

[4] D. Wu and C. Chen, “Colour Visual Cryptography: A Survey," *IEEE Access*, vol. 7, pp. 136014–136032, 2019.

[5] Sundaram, G., Rivera, M., Rivera, M., Wheeler, P., & Pérez Guzmán, R. (2025). Reinforcement Q-Learning-Based Adaptive Encryption Model for Cyberthreat Mitigation in Wireless Sensor Networks. Sensors, 25(7), 2056.