

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 4, Issue 3, December 2024

# Visual Cryptography for Color Image using Digital-Watermarking

Dr. Prasanna Lakshmi Gandi<sup>1</sup>, Pratik Bhaskar Gursal<sup>2</sup>, Mayur Uttam Gaikwad<sup>3</sup>, Rohit Rajendra Gangurde<sup>4</sup>, Ravindra Namdeo Gaikwad<sup>5</sup>

unit Kajenura Gangurue , Kavinura Namueo Gaikwau

Professor, Department of Computer Science and Engineering<sup>1</sup> Students, Department of Computer Science and Engineering<sup>2,3,4,5</sup> Sandip University, Nashik, Maharashtra, India

Abstract: The aim this project is to build secure system for transferring images over the internet. Now internet is the fastest growing way of communication. Data exchange over the internet is increasing day by day, so It is important to secure the transmitted in this medium. Visual cryptography technique can be used to improve the security and privacy of the image by embedding watermark. In visual cryptography encryption of image is done by dividing the image into n number of shares and decryption process is done by combining a certain number of shares or more. Simple visual cryptography is not secure because of the decryption process done by visual system. The information or the image can be retrieved by anyone if the person gets at least some number of shares. Secret images can be reconstructed without any complex computation. In this project we use digital watermarking. Digital watermarking is a technique for inserting secret information into an image. Which enable us to know the source or owner of the copyright

Keywords: Digital Watermarking, Secret Sharing, Encryption, Decryption, Data Security, Image Reconstruction

## I. INTRODUCTION

In the age of digital communication, ensuring the confidentiality, authenticity, and integrity of sensitive visual data has become paramount. Visual cryptography and digital watermarking are two prominent techniques that address these concerns through innovative yet complementary approaches. Visual cryptography provides a robust method for secure image sharing by dividing a secret image into multiple encoded shares, which individually reveal no information but can reconstruct the original image when overlaid. While traditionally limited to binary or grayscale images, advancements have extended its application to color images, posing unique challenges and opportunities due to the complexity of color data.

Simultaneously, digital watermarking has emerged as a key technology for copyright protection, data authentication, and tamper detection by embedding imperceptible yet retrievable information into digital content. The convergence of these two techniques—visual cryptography and digital watermarking—offers a novel framework for enhanced image security, especially in color domains. By embedding a watermark into the cryptographically processed shares, this hybrid approach not only protects sensitive images but also provides an additional layer of verification, ensuring that the reconstructed image is both authentic and secure.

This paper explores the integration of visual cryptography with digital watermarking for color images, focusing on overcoming the challenges of color representation, pixel-level encoding, and efficient reconstruction. The proposed methodology leverages the strengths of both techniques to provide a comprehensive solution for secure image sharing and authentication in applications such as secure communication, digital rights management, and multimedia forensics

#### **Problem Statement**

With the rapid expansion of digital communication and multimedia technologies, the security and authenticity of color image data have become critical concerns. Traditional visual cryptography methods effectively secure grayscale or binary images but face significant challenges when applied to color images due to the increased complexity of color

Copyright to IJARSCT www.ijarsct.co.in DOI: 10.48175/568



# IJARSCT



International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

#### Volume 4, Issue 3, December 2024

representation and processing. Furthermore, while visual cryptography ensures secure sharing, it lacks mechanisms to verify the authenticity of the reconstructed image, making it vulnerable to tampering or unauthorized modifications.

On the other hand, digital watermarking provides robust techniques for embedding authentication and copyright information into images but may not inherently secure the content against interception or unauthorized access. The independent application of these two techniques fails to address the dual challenges of ensuring both the confidentiality and authenticity of sensitive color image data.

This research seeks to address the gap by integrating visual cryptography and digital watermarking into a unified framework for color images. The core challenge lies in efficiently splitting and reconstructing color images while embedding and retaining an imperceptible, robust watermark that ensures the authenticity and integrity of the shared data. Achieving this involves overcoming hurdles such as color channel decomposition, secure encoding, and resistance to noise or data loss during transmission. The proposed solution aims to provide a secure, reliable, and efficient method for protecting color images in sensitive applications such as secure communication, digital rights management, and forensic analysis.

#### **II. PROPOSED SYSTEM**

In order to meet the increasing need for easily accessible healthcare services, particularly in underserved and rural areas, the proposed telemedicine system seeks to offer an integrated platform for remote healthcare delivery. Real-time consultations, secure data management, payment processing, and prescription administration are just a few of the capabilities that the system will include. The architecture is designed to be user-friendly, safe, and scalable so that patients and healthcare professionals may utilize it efficiently.

#### Key features of Proposed System:

#### **Input Image Preparation**

- A color image is selected as the secret image.
- The image is preprocessed using standard techniques like resizing, color normalization, and compression to ensure compatibility with the VC and DW processes.

#### **Visual Cryptography Process**

- The input image is divided into its three primary **RGB color channels**.
- Each channel is then split into **multiple shares** using a modified visual cryptography algorithm designed for color images.
- The generated shares are visually meaningless and securely encrypted, ensuring that the original image cannot be reconstructed from any single share.

#### Watermark Embedding

- A robust watermark (e.g., a logo, authentication code, or unique identifier) is embedded into one or more of the visual cryptographic shares using **digital watermarking techniques**.
- The watermark is imperceptible in the share but can be extracted during the verification process.

#### Share Distribution

• The shares are securely transmitted to the intended recipients over different communication channels to ensure redundancy and minimize interception risks.

#### **Reconstruction and Verification**

- To reconstruct the original image, the authorized recipients combine the shares.
- During reconstruction, the embedded watermark is extracted and verified to confirm the authenticity and integrity of the reconstructed image.

#### **Post-Reconstruction Processing**

• The reconstructed image undergoes a verification step to detect any tampering or unauthorized modifications using the extracted watermark.



## IJARSCT



International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

#### Volume 4, Issue 3, December 2024

## III. SYSTEM ARCHITECTURE

This architecture ensures comprehensive security, authentication, and reliability for sensitive color images, making it suitable for applications such as secure communication, medical imaging, and digital rights management.



Fig 1. Proposed System Architecture

## **IV. CONCLUSION**

This research successfully presents an integrated framework combining Visual Cryptography (VC) and Digital Watermarking (DW) to enhance the security, authenticity, and integrity of color images. The proposed system offers a robust solution for secure image sharing, protecting sensitive data while ensuring the image's authenticity through watermark embedding. By leveraging VC, the system ensures that only authorized parties can access the original content, while the watermarking process provides an added layer of verification, making it resistant to tampering and unauthorized alterations.

The integration of these two techniques specifically addresses the challenges associated with color image cryptography, such as the complexity of handling multiple color channels and the need for seamless reconstruction. Furthermore, the incorporation of watermarking ensures that the image's integrity can be verified during and after transmission, making it suitable for applications in secure communication, copyright protection, and digital forensics.

As digital communication and multimedia applications continue to grow, this hybrid approach lays the foundation for future advancements in secure image transmission and protection. Future work could explore optimizing the watermarking algorithm for even greater imperceptibility and robustness against compression and noise, as well as investigating its scalability for larger datasets or real-time applications. Ultimately, the proposed system offers a comprehensive solution for safeguarding color images against unauthorized access, ensuring both their security and authenticity in a variety of practical scenarios.

## V. ACKNOWLEDGMENT

We extend our sincere gratitude to the Assistant Professor of the Computer Science Engineering Department at Sandip University, Nashik, for her invaluable support and encouragement throughout the course of our research on the publication, "Telemedicine." Her guidance and expertise have played a pivotal role in shaping our study. We would also like to express our heartfelt appreciation to our Director and management for providing us with the essential resources

Copyright to IJARSCT www.ijarsct.co.in DOI: 10.48175/568



# IJARSCT



International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

#### Volume 4, Issue 3, December 2024

and opportunities to undertake this project. Their steadfast support has been crucial to our success. Our deepest thanks go to the staff of the CS department, whose collaboration and assistance have significantly contributed to the completion of this work.

We are grateful for their dedication and willingness to share their knowledge whenever needed. We would also like to acknowledge our respected professors for their guidance and invaluable insights during the course of our research. Their expertise and feedback have greatly enhanced the quality of our study. To our parents, we are profoundly thankful for their unwavering support and encouragement throughout our journey. Their love and motivation have been the driving force behind our achievements.

Lastly, we wish to express our gratitude to all our friends and colleagues who have contributed to the success of this article. Their support, discussions, and contributions have been invaluable. We are sincerely thankful to each individual and organization mentioned above for their significant role in the accomplishment of our study. Without their support, this achievement would not have been possible.

#### REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Proceedings of the Advances in Cryptology - EUROCRYPT '94, Springer, 1995, pp. 1-12.

[2] S. K. Sharma, R. D. Sudhakar, and R. K. Gupta, "A novel visual cryptography technique for color images," International Journal of Computer Science and Network Security, vol. 7, no. 4, pp. 66-70, 2007.

[3] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital watermarking," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1293-1301, 1997.

[4] W. Puech, D. Bolle, and J. C. J. M. de Valk, "Watermarking techniques and applications," Journal of Electronic Imaging, vol. 10, no. 4, pp. 1159-1168, 2001.

[5] R. S. L. Varga, M. W. S. Lin, and B. A. Huber, "A survey of visual cryptography and its applications to color images," Journal of Visual Communication and Image Representation, vol. 23, no. 1, pp. 97-105, 2012.



