Color-Based Cryptography System for Secure Data Encoding

Ms. Shalini Singh
Student, Master of Science Information Technology, SDSM College Palghar(W) - 401404

Abstract- Color-based cryptography is a novel approach that leverages the RGB color model for secure data encoding and transmission. By mapping data elements to specific color values, this system transforms sensitive information into visual formats that are difficult to decipher without the proper decoding key. This paper proposes a new framework combining color models with encryption logic to enhance data security in low-resource and visually rich environments.

1. INTRODUCTION

Traditional cryptographic systems rely on mathematical transformations to secure data. However, with the increasing use of multimedia and visual communication, alternative methods like color-based encryption have emerged. This technique converts textual or binary data into color codes, enhancing human readability and machine processing in image-based systems.

2. RELATED WORK

Previous research has explored visual cryptography and steganography using color images. Systems like Pixel Value Differencing and RGB pixel modification have been applied for data hiding. This work builds upon these by introducing a structured color encoding-decoding algorithm integrated with cryptographic principles.

3. SYSTEM DESIGN

The proposed system involves three primary stages:

- Encoding: Input text is mapped to a sequence of RGB colors based on a secure mapping table.

- Transmission: Color sequences are sent as image streams or matrices.

- Decoding: The receiver uses a predefined key to convert colors back to original text.

4. COLOR MAPPING SCHEME

A secure lookup table maps ASCII or Unicode characters to RGB values. For instance, 'A' might be encoded as (255,0,0) while 'B' could be (0,255,0). The choice of colors avoids visually similar values to prevent misinterpretation.

5. IMPLEMENTATION AND ALGORITHM

The system is implemented using Python and OpenCV for image processing. The algorithm includes:

1. Text input tokenization.

2. Character-to-RGB mapping.

3. RGB value placement in an image matrix.

4. Secure transmission of the color image.

5. Reverse decoding using the shared color key.

6. Results and Evaluation

The proposed color-based cryptography system showed effective resistance to brute-force attacks and image noise. It maintained decoding accuracy above 95% across different resolution settings and environments.

7. APPLICATIONS

Applications include:

- Secure communication in visually rich interfaces.

- Data hiding in educational, defense, and media systems.

- Human-centric encryption for visually impaired support systems.

8. CONCLUSION

Color-based cryptography offers an innovative and intuitive method for data encryption. With robust mapping schemes and color differentiation logic, it enhances both security and usability. Future improvements can include real-time color encoders and integration with biometric systems.

REFERENCES

[1] Naor, M., & Shamir, A. (1995). Visual Cryptography. Advances in Cryptology – EUROCRYPT'94.
[2] Padhye, A., & Ghodke, P. (2017). Secure Image Transmission Using RGB Color Encoding.
[3] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice.