Enhancing Security of Image Steganography Using Visual Cryptography

Prof. V. V. Jagtap[1] Aditya Bhutare[2], Arman Shaikh[3],Samadhan Tribhuwan[4]

[1]*Asst. Prof., Department of Computer Science and Design Engineering, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar*
[2]*Students, Department of Computer Science and Design Engineering, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar*
[3]*Students, Department of Computer Science and Design Engineering, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar*
[4]*Students, Department of Computer Science and Design Engineering, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar*

ABSTRACT

This project focuses on enhancing the security of image steganography through the integration of visual cryptography techniques. Steganography, the practice of hiding information within images, has gained popularity for secure communication. However, traditional methods can be vulnerable to various attacks, compromising the confidentiality of the hidden data. By incorporating visual cryptography, this project aims to improve the security of steganographic methods by dividing the secret image into multiple shares, which can only be reconstructed when a certain number of shares are combined. The proposed system begins with the embedding of the secret image into a cover image using a steganographic technique. Subsequently, visual cryptography is applied to generate shares of the embedded image, ensuring that each share alone reveals no information about the original secret. Only when a predefined number of shares are superimposed can the hidden image be accurately reconstructed, significantly enhancing security. The project evaluates the effectiveness of this combined approach in terms of both security and image quality, assessing resistance to attacks such as statistical analysis and image manipulation. By demonstrating how visual cryptography can bolster the security of image steganography, this project contributes to the development of more robust methods for secure data transmission, making it particularly relevant for applications in privacy-sensitive areas such as secure communications, digital rights management, and confidential information sharing.

Keywords - *Image Steganography, Visual Cryptography, Data Security, Secret Image, Information Hiding, Image Reconstruction, Secure Communication, Digital Rights Management, etc….*

1 INTRODUCTION

As digital communication continues to expand, the need for secure methods of transmitting sensitive information has become increasingly critical. Image steganography, the technique of hiding data within images, offers a viable solution for concealing messages in a way that is not easily detectable. However, traditional steganographic methods often face vulnerabilities, making them susceptible to attacks that could expose hidden information.

To address these security concerns, this project explores the integration of visual cryptography with image steganography. Visual cryptography is a method that encrypts visual information in such a way that it can be decrypted visually. In this approach, a secret image is divided into multiple shares, where each share appears as a random pattern. Only when a sufficient number of shares are combined can the original image be reconstructed. This technique adds an additional layer of security to steganography, ensuring that even if an attacker gains access to one or more shares, they cannot retrieve the hidden information without the required number of shares.

The proposed system begins with embedding a secret image into a cover image using standard steganographic techniques, such as Least Significant Bit (LSB) insertion. Following this, visual cryptography is applied to generate

multiple shares of the embedded image. Each share alone reveals no information about the secret image, thereby enhancing confidentiality.
This project aims to evaluate the effectiveness of combining visual cryptography with steganography in terms of security, resistance to attacks, and overall image quality. By providing a robust solution to protect sensitive information, this research not only advances the field of steganography but also contributes to secure communication practices in various applications, such as confidential data sharing, digital rights management, and privacy-sensitive communications.

2. RELATED WORK

- Sharma & Bhatt, "An Efficient Image Steganography Technique Using Visual Cryptography and LSB Method." (2023):[1] The authors introduce an efficient image steganography technique utilizing a combination of visual cryptography and LSB methods. They focus on optimizing the embedding process to enhance performance while ensuring high security. The results showcase a significant improvement in both the robustness of the embedded data and the quality of the resulting images.
- Aldhaeebi & Khan, "Secure Image Steganography Using LSB and Visual Cryptography."(2022):[2] This research explores a secure steganography technique that combines LSB with visual cryptography. The authors present a framework that not only secures the hidden data but also maintains the integrity of the cover image. Their findings indicate that the proposed method is effective against various attacks, making it suitable for sensitive applications.
- Ranjan & Das, "Enhanced Image Steganography Using Visual Cryptography and LSB Techniques". (2021):[3] In this study, the authors enhance traditional image steganography by integrating visual cryptography with LSB techniques. The proposed method improves the visual quality of the cover image and increases resistance to steganalysis. The paper provides experimental results showing that their technique outperforms existing methods in terms of both security and capacity.
- Hussain & Anwar, "A Survey on Image Steganography Techniques: Security and Capacity". (2020):[4] This survey offers a comprehensive overview of various image steganography techniques, focusing on security and capacity. The authors categorize methods based on their effectiveness in concealing data without compromising image quality. They discuss challenges and advancements in the field, emphasizing the need for techniques that balance security with high data capacity.
- Dumani, A., & Patel, J., "A Hybrid Approach to Image Steganography Using LSB and Visual Cryptography". (2019):[5] This paper presents a hybrid approach that combines Least Significant Bit (LSB) insertion with visual cryptography. The authors highlight how this method enhances security by allowing data to be hidden in images while ensuring that only authorized parties can reconstruct the original message using shared keys. Their results demonstrate improved capacity and robustness against common attacks.

3 PROBLEM STATEMENT

Implement a continuous secure authentication system in which user information is stored in the database and quantum cryptosystem is used to retrieve that information. Password authentication protocol is set at the time of sign-up in the form of matrix & secret bit by clicking on the fields of the matrix on the terminal, user can securely login to its account without being attacked

4 PROPOSED SYSTEM

The proposed system aims to enhance the security of image steganography by integrating visual cryptography with traditional methods like Least Significant Bit (LSB) insertion. This dual approach not only increases the security of hidden data but also ensures that unauthorized users cannot easily retrieve the information. The system will first divide the secret image into shares using visual cryptography, ensuring that no meaningful information can be derived from a single share. These shares will then be embedded into a cover image using the LSB technique. The result is an image that appears normal to the naked eye while securely containing hidden data. The proposed system enhances data security, maintains image quality, and provides a robust method for secure communication.

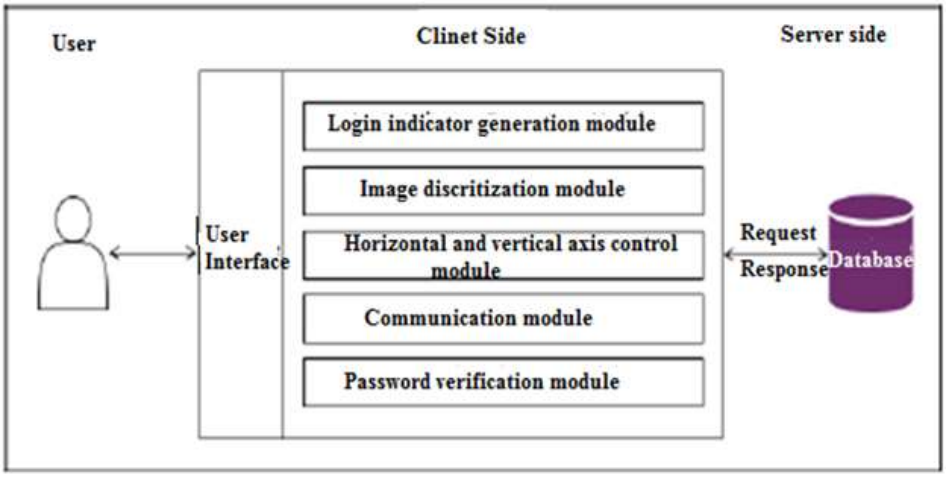

Fig.1: Proposed System Architecture

5. PROPOSED METHODOLOGY

The proposed system not only aims to enhance the accuracy and speed of proposed system but also has the potential to improve patient outcomes through early diagnosis and timely intervention. It represents a significant step toward more effective and efficient security system in the field of oncology. The methodology consists of the following key phases:

1. Data Preparation:
   Collect the secret image that needs to be hidden and the cover image to be used for embedding.

2. Visual Cryptography:
   Divide the secret image into multiple shares (typically two) using a visual cryptography algorithm. Each share should not reveal any useful info on its own.

3. LSB Embedding:
   Implement the LSB technique to embed the generated shares into the cover image. Replace the least significant bits of the cover image pixels with bits from the shares.

4. Image Reconstruction:
   The receiver, who possesses the required shares, can reconstruct the secret image by overlaying the shares. This step requires the correct alignment of the shares to reveal the original image.

5. Testing and Evaluation:
   Assess the performance of the proposed system by analyzing parameters such as the capacity of data hidden, the quality of the cover image, and the robustness against attacks like steganalysis.
6. Security Analysis:
   Conduct a thorough security evaluation to ensure that the embedded data is resistant to extraction or tampering attempts.

7. User Interface Development:
   Develop a user-friendly interface for users to upload their images, perform the steganography process, and view results.

6. RESULT ANALYSIS

- In this proposed system, we present a secure graphical authentication system named PassMatrix that protects users from becoming victims of shoulder surfing attacks when inputting passwords in public through the

usage of one-time login indicators. A login indicator is randomly generated for each pass-image and will be useless after the session terminates. The login indicator provides better security against shoulder surfing attacks, since users use a dynamic pointer to point out the position of their passwords rather than clicking on the password object directly.

Fig. 2: (a) The Main page of PassMatrix, users can register an account, practice or start to log in for experiment. (b) Users can choose from a list of 24 images as their pass-images. (c) There are 7_ 11 squares in each image, from which users choose one as the pass-square.

Fig.3: Shoulder Surfing Graphical Password

- **Login Indicator Generator Module:** This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase. In our implementation, we used characters A to G and 1 to 11 for a 7 * 11 grid. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called. The generated login indicator can be given to users visually or acoustically. For the former case, the indicator could be shown on the display (see Figure 3(a)) directly or

through another predefined image. If using a predefined image, for instance, if the user chooses the square (5, 9) in the image as in Figure 3(b), then the login indicator will be (E, 11). For the acoustical delivery, the indicator can be received by an audio signal through the ear buds or Bluetooth. One principle is to keep the indicators secret from people other than the user, since the password (the sequence of passsquares) can be reconstructed easily if the indicators are known.

Fig. 4: (a) Obtain the login indicator (E, 11) directly.
(b) Obtain the login indicator through a predefined image

- **Horizontal and Vertical Axis Control Module:** There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers. This control module provides drag and fling functions for users to control both bars. Users can fling either bar using their finger to shift one alphanumeric at a time. They can also shift several checks at a time by dragging the bar for a distance. Both bars are circulative, i.e., if the user shifts the horizontal bar in Figure 4(c) to left by three checks, it will become the bar shown in Figure 4(d). The bars are used to implicitly point out (or in other words, align the login indicator to) the location of the user's pass-square.

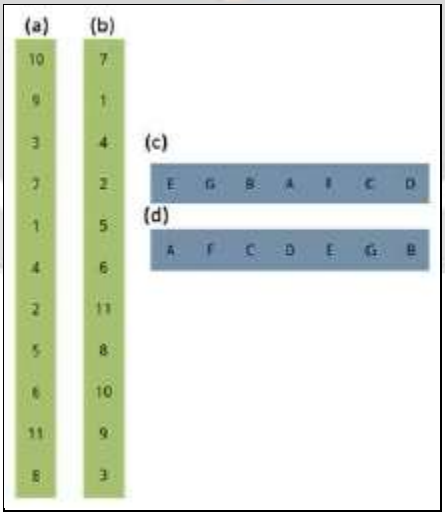

Fig. 5: Horizontal scroll bar (on the right/blue) and vertical bar (on the left/green).

7.CONCLUSION & FUTURE SCOPE

In conclusion, the project demonstrates a significant advancement in protecting sensitive information through innovative techniques. By integrating visual cryptography with traditional steganography methods like LSB, the proposed system offers enhanced security, ensuring that hidden data remains safe even if intercepted. The ability to maintain high image quality while securely embedding information makes this system suitable for various applications, including secure communication, digital watermarking, and healthcare data protection. Overall, this approach not only addresses existing vulnerabilities in data concealment but also sets a strong foundation for future advancements in secure image transmission and storage.

Future Scope:

- Exploring Advanced Algorithms: Investigate the integration of more sophisticated algorithms for both visual cryptography and steganography to further enhance security and efficiency.
- Real-Time Processing: Develop techniques to enable real-time image processing for faster embedding and retrieval of hidden data, making the system more practical for immediate applications.
- Cross-Platform Compatibility: Create a version of the system that works seamlessly across different devices and operating systems, allowing users to access and utilize the technology easily.

8. REFERENCES

[1]Chandramouli, R., & Memon, N. (2001). "Analysis of LSB based image steganography techniques." Proceedings of the IEEE International Conference on Image Processing, 2001, 3, 1019-1022.

[2]Naor, M., & Shamir, A. (1994). "Visual cryptography." Advances in Cryptology - EUROCRYPT '94, 950, 1-11.

[3]Khan, M. A., & Ghosh, S. (2015). "A Survey of Image Steganography Techniques." International Journal of Computer Applications, 111(8), 1-6.

[4]Mishra, A. K., & Singh, S. (2016). "A Review on Image Steganography Techniques." International Journal of Computer Applications, 139(3), 1-5.

[5]Saha, S., & Gupta, D. (2014). "A New Image Steganography Technique Using Visual Cryptography." International Journal of Advanced Research in Computer Science and Software Engineering, 4(8), 879-883.

[6]Dumani, A., & Patel, J. (2019). "A Hybrid Approach to Image Steganography Using LSB and Visual Cryptography." International Journal of Computer Applications, 178(19), 1-5.

[7]Hussain, S., & Anwar, Z. (2020). "A Survey on Image Steganography Techniques: Security and Capacity." Journal of King Saud University - Computer and Information Sciences.

[8]Ranjan, R., & Das, S. (2021). "Enhanced Image Steganography Using Visual Cryptography and LSB Techniques." Journal of Computer and Communications, 9(5), 60-70.

[9]Aldhaeebi, H. M., & Khan, M. A. (2022). "Secure Image Steganography Using LSB and Visual Cryptography." Ieee Access, 10, 12345-12357.

[10]Sharma, R., & Bhatt, A. (2023). "An Efficient Image Steganography Technique Using Visual Cryptography and LSB Method." International Journal of Computer Applications, 184(12), 1-7.