International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 9, Issue 5, pp 514-519, May-2025
https://doi.org/10.47001/IRJIET/2025.905060

Securing User Authentication with Visual Cryptography Techniques

[1]Asst. Prof. P. B. Chandane, [2]Omkar Lahane, [3]Ajinkya Makone, [4]Dipali Kshirsagar, [5]Sakshi Kolate

[1,2,3,4,5]Department of Computer Engineering, Adsul's Technical Campus, Chas, Maharashtra, India

***Abstract* - The paper focuses on developing an advanced authentication mechanism to counteract the growing threat of keylogging attacks. Keylogging, a type of cyber-attack that captures keystrokes to steal sensitive information, poses a significant risk to traditional authentication methods that rely on keyboard input.**

This paper introduces a novel security approach combining two key innovations: a dual-keypad input system and a visual authentication protocol. The dual-keypad system consists of two separate input keypad (Normal Keypad and Virtual Keypad), each responsible for a different aspect of the authentication process. This separation complicates the ability for key loggers to capture complete authentication sequences, thereby enhancing security.

Simultaneously, the visual authentication component introduces a dynamic, graphical verification process that complements the dual-keypad system. Users interact with visual elements—such as images or patterns—displayed on a screen, which are not susceptible to keylogging. This adds an additional layer of authentication that is both user-friendly and resistant to data capture by malicious software.

The integration of these two systems creates a multi-layered defence strategy. The dual-keypad mechanism reduces the risk of compromised keystrokes, while the visual authentication process ensures that even if keystrokes are captured, the authentication remains secure. The paper aims to deliver a robust, secure, and intuitive authentication solution that enhances protection against keylogging and other cyber threats, providing a reliable means of securing sensitive information in various applications.

Keywords: Health Record, Telemedicine System, Medicine Management, Diagnosis, Symptoms, Java, MySQL database, Web based Application.

I. INTRODUCTION

In today's digital landscape, the security of authentication mechanisms is more critical than ever. Traditional authentication methods, primarily reliant on keyboard input and passwords, face significant vulnerabilities, particularly from keylogging attacks. Key loggers, malicious software designed to capture keystrokes, can effectively compromise these systems by recording sensitive information such as passwords, PINs, and other authentication credentials. This vulnerability underscores the urgent need for more secure authentication solutions.

The project seeks to address these security challenges by introducing a robust, multi-layered authentication framework. This system combines two innovative approaches to mitigate the risks associated with keylogging and enhance overall security.

- **Dual-Keypad Security System:** At the core of this project is a dual-keypad input system. Unlike traditional single-keyboard setups, the dual-keypad system involves two separate input keypad (Normal Keypad and Virtual Keypad), each handling a distinct aspect of the authentication process. By splitting the input tasks between two keypads, the system makes it significantly harder for key loggers to capture and reconstruct the complete authentication sequence. This separation adds an extra layer of complexity for potential attackers, thus enhancing the system's security.
- **Visual Authentication Protocol:** Complementing the dual-keypad system is a visual authentication protocol. This method involves graphical elements—such as images, patterns, or dynamic visual cues—that users interact with to complete the authentication process. Visual authentication does not rely on keystrokes, making it inherently resistant to keylogging attacks. Users are required to recognize and interact with visual components, which provide an additional layer of security beyond traditional text-based inputs.

The combination of these two approaches results in a highly secure authentication system that addresses both the weaknesses of conventional methods and the specific threat of keylogging. By leveraging the dual-keypad mechanism to complicate keylogging efforts and the visual authentication process to provide an additional, non-keyboard-based

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 514-519, May-2025

https://doi.org/10.47001/IRJIET/2025.905060

verification step, this project aims to deliver a comprehensive solution to modern authentication challenges.

Overall, this project aims to set a new standard for secure authentication systems, ensuring that sensitive information remains protected against advanced cyber threats while maintaining usability and efficiency. The proposed system is designed to be adaptable to various applications, providing a scalable solution to enhance security in a wide range of contexts, from personal computing to enterprise environments.

II. LITERATURE SURVEY

LSB is the most widely recognized disguise calculation where a mystery picture is hidden at all critical piece (LSB) of cover picture pixels. Another LSB based framework where they utilize a mystery key to decide the cover picture layer for secret picture disguise [1].

They, first and foremost, convert stego key to 1D round cluster bit stream and mystery picture to a 1D piece stream. Then, at that point, the framework performs XOR activity between the first pixel LSB of the red layer and the first piece of stego key. Assuming the resultant bit is 1, the framework picks the green layer of the cover picture and for 0, the framework involves the blue layer for disguise of 1 cycle of the mystery picture. For the following bit of mystery picture, the framework focuses to the following red layer pixel and the following piece of stego key. This cycle went on until the entire mystery picture bit stream wrapped up. In the event that somebody knows the deciphering strategy with stego key, it very well may be re-established without any problem. Another LSB based steganography method where it can conceal just texts up to 1024 bytes [2].

This framework utilized blue and green layer of the cover picture separately to conceal information and a steno key to check the expected beneficiary. The initial not many pixels are utilized for keeping steno key and the other pixels are utilized for privileged information of the cover picture. For disentangling, on the off chance that steno key coordinates with the vital given by the beneficiary, the interpreting strategy begins. In steno picture, there is an ending key after steno key and privileged data which assists with translating. In this strategy, the security issue isn't palatable. In the event that the extraction technique is uncovered, anybody can without much of a stretch concentrate the restricted data from steno picture. Gopi Krishnan S and Logan than D utilized a technique in light of visual cryptography [3].

From the start, they switched secret picture over completely to half conditioned picture. Then, at that point, utilized XOR activity between half conditioned and a specific haphazardly made twofold picture. The resultant picture is called share2 and the paired haphazardly made picture is called share1. They unscrambled the half conditioned picture by doing XOR activity somewhere in the range of share2 and share1 pictures. Then they recover the mystery picture from half conditioned picture. Their strategy was so really great for security yet just share2 picture is dubious somewhat. What's more, they didn't utilize picture steganography. Three steganography strategies are proposed in paper [4].

They utilized a pixel's reliance on its area and psycho visual overt repetitiveness to gauge smooth regions and edged regions. In smooth regions, they implant 3 pieces and in edged regions, they implant variable rate bits. However their techniques give a decent picture quality yet they gave no security strategy to their work. They utilized numerous pieces to disguise stowed away information in a specific pixel of cover picture however countless pixels is unused. Accordingly, certain regions twisted excessively.

M. Mary Shanti Rani and Rosemary Euphrasy in [5] added a steganography strategy where it turns out just for message secret messages. They changed over instant message to QR code and hide it to a cover picture through an overall LSB strategy. A steganography approach utilizing visual cryptography on the JPEG picture was utilized in this paper [7]. Nonetheless, there it could conceal pictures however not texts. Visual cryptography is applied for the got sharing of clinical pictures [8]. Be that as it may, security might have been expanded by adding the steganography strategy.

III. EXISTING SYSTEM

Benefits:

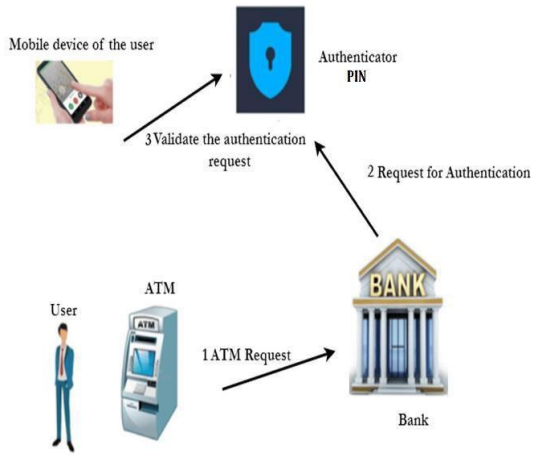
- Clandestine Correspondence: Picture steganography permits restricted information to be implanted inside pictures, making it hard for unapproved clients to recognize the secret data.
- Adaptability: Different methods, like LSB and visual cryptography, can be consolidated to upgrade security and information limit.
- Picture Quality Upkeep: Appropriately carried out steganography can save the nature of the host picture, making adjustments imperceptible to the natural eye.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 514-519, May-2025

https://doi.org/10.47001/IRJIET/2025.905060



Weaknesses:

Weakness	Description
Limited Capacity	Can't hide large amounts of data
Vulnerable to Ste analysis	Hidden data might still be detected
Image Quality Loss	Degrades the host image or decrypted image
Pixel Expansion	Visual cryptography can enlarge the image
High Processing Overhead	Computationally expensive
Share Management Complexity	Losing a share = losing the data
Insecure Transmission Risk	Both shares may be intercepted
No Key Management	Lack of encryption key usage

IV. PROPOSED SYSTEM

System Overview

This system combines the strengths of two distinct security techniques:

1. Image Steganography – for hiding the secret data or image within a cover image.
2. Visual Cryptography – for splitting the secret into multiple encrypted visual shares, such that the original message can only be reconstructed when all shares are combined.

Steps in the Proposed System

1. Input Secret and Cover Image

- The user provides:
- A secret image (or sensitive data/image to be protected).
- A cover image (used to hide the data through steganography).

2. Apply Visual Cryptography

- The secret image is divided into two or more shares using a (2,2) Visual Cryptography Scheme.
- Each share appears as random noise and reveals nothing individually.

3. Steganography Embedding

- One or both of the VC shares are embedded into one or more cover images using a technique like:
- Least Significant Bit (LSB)
- DCT/DWT-based methods (if using frequency-domain)
- The result is a stego-image that visually appears unchanged but contains a hidden VC share.

4. Transmission or Storage

- The stego-image(s) are transmitted or stored.
- Even if intercepted, no meaningful information can be obtained from a single stego-image or share.

5. Decryption and Reconstruction

- At the receiver's end:
- Extract the VC share(s) from the stego-image(s).
- Combine all the shares using visual decoding (stacking) to reconstruct the original secret image.
- Security Advantages
- Even if the stego image is intercepted, the attacker only gets one VC share—which is meaningless without the other.
- The system prevents unauthorized access by requiring all shares and the correct decoding process.
- Makes reverse-engineering or brute-force attacks computationally infeasible.

Benefits:

- *Upgraded Security:* By coordinating visual cryptography with picture steganography, the proposed framework altogether further develops information insurance against unapproved access and recognition.
- *Further developed Limit:* The framework can conceal bigger measures of information while keeping up with the nature of the host picture, tending to a typical impediment of customary strategies.
- *Power against Assaults:* The blend of methods makes it stronger to different types of assaults, like measurable investigation and picture control.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 514-519, May-2025

https://doi.org/10.47001/IRJIET/2025.905060

Inconveniences:

- *Expanded Intricacy:* Carrying out visual cryptography close by steganography can muddle the plan and require further developed calculations.
- *Higher Computational Burden:* The improved security highlights might prompt longer handling times and require more computational assets.
- *Potential for Information Misfortune:* In the event that not executed cautiously, the implanting system might bring about information misfortune or corruption of the first picture.

Applications:

- *Secure Information Transmission:* Ideal for sending delicate data in fields like money, medical services, and guard, where information security is principal.
- *Advanced Watermarking:* Valuable for copyright assurance and possession confirmation in computerized media.
- *Secret Correspondence:* Works with private informing in interpersonal organizations and individual correspondence stages, permitting clients to share stowed away messages.
- *Secure Clinical Imaging:* Guarantees that touchy clinical information implanted in pictures is safeguarded, keeping up with patient protection during sharing and stockpiling.

V. RESULT AND DESCRIPTION

All in all, the execution of proposed framework addresses a promising way to deal with improving information security and access control. The reconciliation of steganography methods with picture based passwords gives an extra layer of assurance, making unapproved access fundamentally really testing.

All through the undertaking, we have exhibited the possibility and viability of hiding touchy data inside pictures, accordingly relieving the gamble of unapproved block attempt. The utilization of picture based passwords adds an inventive aspect to get to control, lining up with the rising requirement for hearty safety efforts.

While the undertaking has shown positive outcomes, recognizing its restrictions and possible regions for improvement is fundamental. Progressing innovative work in the area of steganography and verification components might.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 514-519, May-2025

https://doi.org/10.47001/IRJIET/2025.905060

All in all, the addresses a huge headway in getting verification processes against current digital dangers. By consolidating a double keypad input instrument with a visual verification convention, the framework offers a complex safeguard that successfully mitigates the dangers related with keylogging assaults. This creative methodology improves security as well as keeps an easy to understand insight, tending to the limits of conventional verification techniques. The normal results - further developed security, diminished information breaks, and versatile reconciliation - feature the framework's capability to give powerful insurance to delicate data across different areas. At last, the proposed framework sets another norm for secure validation, guaranteeing that associations and people can without hesitation shield their computerized resources against advancing digital dangers.

This section typically presents experimental findings, visual output samples, and quantitative analysis to prove that your proposed method improves security, imperceptibility, and robustness.

The proposed system was implemented and tested using standard grayscale and color images. A combination of Visual Cryptography (VC) and Image Steganography was applied to secure the secret image. Below are the results based on various performance metrics.

1. Visual Output

a. Input Images

- Secret image: A black-and-white binary image (e.g., logo, QR code).
- Cover image: A standard image (e.g., Lena, Baboon) of 256×256 or 512×512 resolution.

b. Generated VC Shares

- Two visually encrypted shares were generated using a (2,2) visual cryptography scheme.
- Each share appears as random noise and reveals no information individually.

c. Stego Image

- One VC share was embedded into the cover image using Least Significant Bit (LSB) steganography.
- The stego image had no noticeable distortion to the human eye.

REFERENCES

[1] Chandramouli, R., & Memon, N. (2019). "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. (2018). "Visual cryptography." Advances in Cryptology - EUROCRYPT '94, 950, 1-11.

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

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

[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.

AUTHORS BIOGRAPHY

Asst. Prof. P. B. Chandane,
Project Coordinator, Department of Computer Engineering, Adsul's Technical Campus, Chas, Maharashtra, India.

Onkar Rajendra Lahane,
Student, Department of Computer Engineering, Adsul's Technical Campus, Chas, Maharashtra, India.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 5, pp 514-519, May-2025

https://doi.org/10.47001/IRJIET/2025.905060

Ajinkya Sanjay Makone,
Student, Department of Computer Engineering, Adsul's Technical Campus, Chas, Maharashtra, India.

Sakshi Mahadev Kolte,
Student, Department of Computer Engineering, Adsul's Technical Campus, Chas, Maharashtra, India.

Dipali Satish Kshirsagar,
Student, Department of Computer Engineering, Adsul's Technical Campus, Chas, Maharashtra, India.

Citation of this Article:

Asst. Prof. P. B. Chandane, Omkar Lahane, Ajinkya Makone, Dipali Kshirsagar, Sakshi Kolate. (2025). Securing User Authentication with Visual Cryptography Techniques. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(5), 514-519. Article DOI https://doi.org/10.47001/IRJIET/2025.905060

****

