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

ISSN (online): 2581-3048

Volume 8, Issue 11, pp 162-166, November-2024

https://doi.org/10.47001/IRJIET/2024.811017

Enhancing Security of Image Steganography using Visual Cryptography

[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 undertaking centers around fostering a high level confirmation system to neutralize the developing danger of keylogging assaults. Keylogging, a sort of digital assault that catches keystrokes to take delicate data, represents a huge gamble to conventional confirmation techniques that depend on console input. This undertaking presents an original security approach joining two key developments: a double keypad input framework and a visual verification convention. The double keypad framework comprises of two separate information keypad (Ordinary Keypad and Virtual Keypad), each liable for an alternate part of the validation interaction. This division confuses the capacity for keyloggers to catch total confirmation arrangements, accordingly improving security. At the same time, the visual validation part presents a dynamic, graphical check process that supplements the double keypad framework. Clients interface with visual components like pictures or examples showed on a screen, which are not vulnerable to keylogging. This adds an extra layer of validation that is both easy to use and impervious to information catch by malignant programming. The mix of these two frameworks makes a diverse guard technique. The double keypad component decreases the gamble of compromised keystrokes, while the visual validation process guarantees that regardless of whether keystrokes are caught, the verification stays secure. The venture expects to convey a hearty, secure, and natural verification arrangement that improves assurance against keylogging and other digital dangers, giving a dependable method for getting delicate data in different applications.**

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

I. INTRODUCTION

In the present advanced scene, the security of confirmation components is more basic than any time in recent memory. Conventional confirmation strategies, essentially dependent on console information and passwords, face huge weaknesses, especially from keylogging assaults. Keyloggers, malevolent programming intended to catch keystrokes, can successfully think twice about frameworks by recording delicate data like passwords, PINs, and other confirmation qualifications. This weakness highlights the critical requirement for safer verification arrangements.

The task looks to address these security challenges by presenting a hearty, multifaceted verification structure. This framework joins two inventive ways to deal with moderate the dangers related with keylogging and upgrade in general security.

- Double Keypad Security Framework: At the center of this task is a double keypad input framework. Not at all like customary single-console arrangements, the double keypad framework includes two separate information keypad (Ordinary Keypad and Virtual Keypad), each taking care of a particular part of the verification interaction. By dividing the information errands between two keypads, the framework makes it fundamentally harder for keyloggers to catch and recreate the total verification succession. This detachment adds an additional layer of intricacy for likely aggressors, hence upgrading the framework's security.
- Visual Confirmation Convention: Supplementing the double keypad framework is a visual verification convention. This strategy includes graphical components like pictures, examples, or dynamic obvious prompts that clients associate with to finish the verification cycle. Visual confirmation doesn't depend on keystrokes, making it innately impervious to keylogging assaults. Clients are expected to perceive and communicate with visual parts, which give an extra layer of safety past customary text-based inputs.

The blend of these two methodologies brings about an exceptionally safe validation framework that tends to both the shortcomings of customary strategies and the particular danger of keylogging. By utilizing the double keypad instrument to muddle keylogging endeavors and the visual confirmation cycle to give an extra, non-console based check step, this task expects to convey a thorough answer for current verification challenges.

Generally, this undertaking means to set another norm for secure validation frameworks, guaranteeing that delicate data stays safeguarded against cutting edge digital dangers while

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

ISSN (online): 2581-3048

Volume 8, Issue 11, pp 162-166, November-2024

https://doi.org/10.47001/IRJIET/2024.811017

keeping up with convenience and proficiency. The proposed framework is intended to be versatile to different applications, giving an adaptable answer for improve security in a great many settings, from individualized computing to big business conditions.

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 stego key to check the expected beneficiary. The initial not many pixels are utilized for keeping stego key and the other pixels are utilized for privileged information of the cover picture. For disentangling, on the off chance that stego key coordinates with the vital given by the beneficiary, the interpreting strategy begins. In stego picture, there is an ending key after stego 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 stego picture. Gopi Krishnan S and Loganathan 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 Shanthi Rani and K.Rosemary Euphrasia 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.

Weaknesses:

- Weakness to Assaults: Existing frameworks can be vulnerable to discovery through factual examination or control of the picture, taking a chance with openness of the secret information.
- Restricted Limit: how much information that can be concealed without corrupting picture quality is in many cases obliged, especially in essential steganographic procedures.
- Computational Intricacy: A few high level procedures might require critical computational assets, making them less functional for continuous application.

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

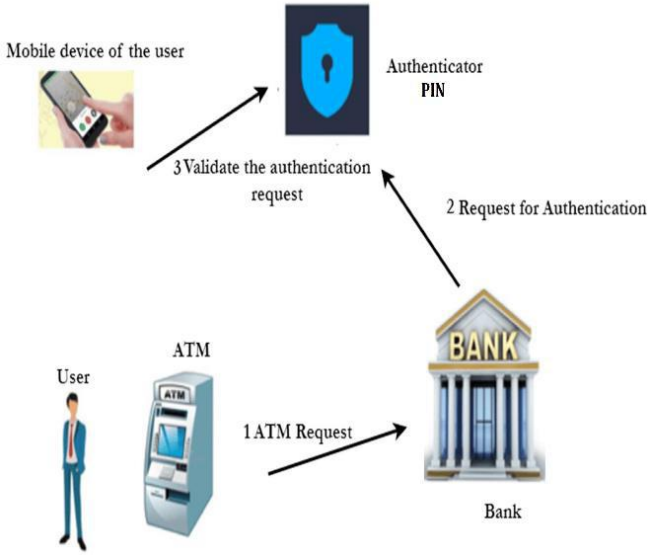
ISSN (online): 2581-3048

Volume 8, Issue 11, pp 162-166, November-2024

https://doi.org/10.47001/IRJIET/2024.811017

Application:

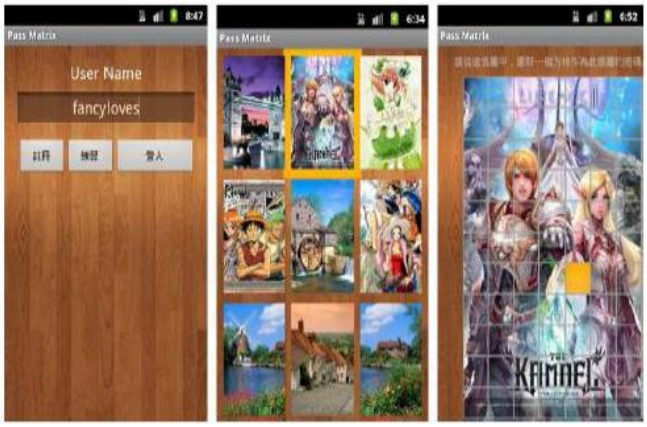
- Secure Correspondence: Utilized in military and administrative interchanges to safely send delicate data.
- Computerized Watermarking: Utilized in copyright assurance, permitting creators to implant proprietorship data inside their advanced substance.
- Clinical Imaging: Works with the solid sharing of clinical information and pictures while keeping up with patient secrecy.
- Web-based Entertainment: Empowers clients to share stowed away messages or information inside pictures without making others aware of their presence.



IV. PROPOSED SYSTEM

The proposed framework improves the security of picture steganography by incorporating visual cryptography with conventional inserting strategies. Initial, a mystery picture is implanted inside a cover picture utilizing strategies like Least Huge Piece (LSB) inclusion. In the wake of implanting, visual cryptography is applied to partition the inserted picture into numerous offers, guaranteeing that each offer alone uncovers no data about the secret information.

To recreate the mystery picture, a predefined number of offers should be consolidated, making it almost inconceivable for assailants to separate the data without admittance to every single required share. This double layer approach essentially helps security, safeguarding touchy data regardless of whether the cover picture is compromised. Furthermore, the framework expects to keep up with high picture quality, guaranteeing that the cover picture remains outwardly imperceptible while giving vigorous information security.



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.

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,

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

ISSN (online): 2581-3048

Volume 8, Issue 11, pp 162-166, November-2024

https://doi.org/10.47001/IRJIET/2024.811017

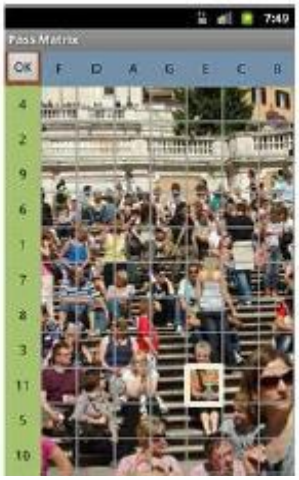
keeping up with patient protection during sharing and stockpiling.

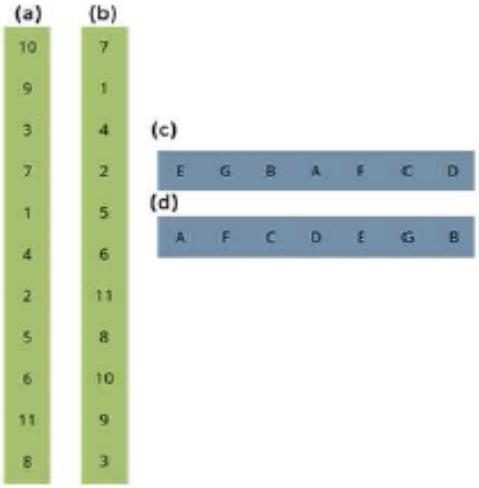
V. RESULT AND DESCRIPTION

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 additionally refine and reinforce the proposed framework.





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.

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.

ISSN (online): 2581-3048
Volume 8, Issue 11, pp 162-166, November-2024
https://doi.org/10.47001/IRJIET/2024.811017

AUTHORS BIOGRAPHY

Asst. Prof. P. B. Chandane,
Project Coordinator, 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.

Omkar Rajendra Lahane,
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.

Ajinkya Sanjay Makone,
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. (2024). Enhancing Security of Image Steganography using Visual Cryptography. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 8(11), 162-166. Article DOI https://doi.org/10.47001/IRJIET/2024.811017

****

