International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 21 No. 3 (1) 2025

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 21, No. 3(1), 2025

Research Paper

SECURING IMAGES WITH AES AND VISUAL CRYPTOGRAPHY TECHNIQUES

[1] V.HARSHAVARDHAN,[2] R.MALATHI,[3] K.PRUTHIVEER,[4] B.SOMASHEKAR,[5] Mr. T. JAYA RAJAN

[1234] Students, [5] Assistant Professor

Department Of Computer Science and Design

Teegala Krishna Reddy Engineering College, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

As the volume of digital communication expands, the demand to protect sensitive information from sophisticated cyber threats has become critical. While encryption and steganography are widely adopted for data security, each has limitations when used in isolation. Encryption transforms data into unreadable ciphertext, securing content but often signaling the presence of confidential information. In contrast, steganography conceals the very existence of a message within media files, though predictable embedding can make it vulnerable to steganalysis. To address these challenges, this project introduces a hybrid model that integrates both techniques for a layered security approach. The secret message is first encrypted using the AES algorithm with a user-defined key, ensuring strong content protection. This encrypted output is then embedded into a cover image using a modified LSB technique, where only one color channel per pixel is altered, minimizing visual distortion. Natural-noise images are preferred to mask hidden data effectively against detection. The proposed system offers rapid encryption, embedding, and decryption, ensuring efficiency with minimal resource usage. It has practical use cases in secure communication, protected file storage, healthcare, defense, and personal privacy. The modular design also allows future improvements, such as dynamic key handling, adaptive embedding based on image features, and integration with cloud platforms for enhanced scalability and redundancy.

Received: 10-7-2025 Accepted: 18-8-2025 Published: 25-8-2025

I. INTRODUCTION

The rapid-fire elaboration of technology and the wide use of the internet have converted how individualities and associations partake information as more sensitive data is changed over digital networks the need for strong security mechanisms has come critical traditional encryption ways cover data confidentiality but do nt hide the presence of communication itself which may still draw attention from vicious actors also introductory steganography ways can conceal information but are decreasingly vulnerable to discovery through ultramodern analysis tools to overcome these limitations the proposed system combines the power of advanced encryption standard aes encryption with least significant bit lsb steganography the translated communication is securely bedded into a cover image without conspicuous changes icing both confidentiality and covert this binary- layered approach significantly enhances the security and sequestration of sensitive data making it largely suitable for secure communication in high- threat surroundings

1.1 Motivation

In today's profoundly interconnected computerized world the transmission of private and touchy data over open systems has gotten to be greatly common in any case this developing reliance on online communication too brings an expanded chance of information breaches cyber-attacks and unauthorized get to customary security components like

fundamental encryption are not adequate on their possess as aggressors proceed to create more progressed strategies to bypass guards to address these dangers combining encryption with steganography gives a multi-layered security approach by stowing away scrambled information interior pictures this framework points to guarantee that indeed on the off chance that the information is captured its presence remains concealed our inspiration is to plan a framework that equalizations solid security straightforwardness and negligible asset utilization making it commonsense for real-world applications

1.2 Problem Statement

Secure communication over the web proceeds to be a major challenge due to the fast progression of hacking methods existing encryption and steganography strategies frequently drop brief as encryption alone gives as it were a single layer of defense and gets to be defenseless in case the key is compromised essentially conventional steganography procedures that utilize unsurprising implanting designs are progressively perceptible through present day steganalysis devices the need of an coordinates multi-layered security approach highlights the require for a framework that not as it were scrambles touchy information but moreover conceals its nearness viably subsequently fortifying generally information assurance against modern cyber dangers

1.3 Scope and Objective Scope:

This research focuses on enhancing secure data transmission using a crypto-steganographic model. The scope includes:

1. Developing a system that allows highly secure communication over untrusted networks.
2. Applying the method to cloud security, military communication, and online transactions where data confidentiality is critical.
3. Extending the approach to various media formats such as audio and video steganography in future implementations.
4. Reducing the risk of steganographic attacks through pseudo-random embedding and noise-based data hiding techniques.

Objective

The primary objectives of this study are:

1. To develop a hybrid security system that ennice raasures both encryption and hidden communication.
2. To introduce a pseudo-randomized embedding technique that prevents steganalysis attacks.
3. To improve the security of data transmission in environments prone to hacking and cyberattacks.
4. To minimize the computational overhead of encryption while maintaining strong security.
5. To ensure confidentiality, integrity, and availability of sensitive information.

II. LITERATURE SURVEY

Feng Li designed a framework that systematically analyzed various shilling attacks and their detection mechanisms in collaborative filtering recommender systems. His system emphasized identifying key traits in injected profiles to enhance detection accuracy. The study provided a classification of attack models and detection attributes, helping to lay the groundwork for building more robust defenses against profile injection attacks.

Thomas Ngo-Ye developed a system that utilized Regressional ReliefF-enhanced text mining techniques to assess the helpfulness of online reviews. By selecting meaningful features from customer reviews and applying regression models, his system successfully identified influential reviews, thus improving information filtering in e- commerce platforms.

Da-Wen Jia, Cheng Zeng, Zhi-Yong Peng, and Peng Cheng proposed an automatic group generation method based on users' shared interests in social media platforms. Their system focused on clustering users who displayed similar preferences toward content elements, forming Common Preference Groups (CPGs) for efficient content sharing

and recommendation.

Su et al. introduced the concept of group shilling attacks, highlighting two main scenarios where attackers either mixed biased ratings with normal behavior or collaborated through organized gray groups to target multiple items. Their work emphasized the complexity and threat level of group-based manipulations in recommendation systems.

Bryan Mehta and Wolfgang Nejdl proposed an unsupervised strategy for detecting shilling attacks by applying principal component analysis (PCA) on user rating profiles. Their system identified anomalous profiles based on their deviation from the normal user behavior, enabling early detection without the need for labeled training data.

Wang et al. developed a group shilling attack detection system that enhanced traditional individual attack detection features. Their method ranked candidate groups using principal component analysis after manually labeling groups with high minimum support, successfully identifying collusive attacks with high similarity among attackers.

Williams, Mobasher, and Burke created a detection system that analyzed the obfuscation tactics used in shilling attacks. Their approach relied on clustering techniques to identify hidden attack profiles and proposed methods to enhance recommender system resilience through robustness against sophisticated attackers.

EXISTING SYSTEM

Over the a long time a few strategies have been created to guarantee secure information transmission over advanced systems the two most common approaches are cryptography and steganography standalone cryptography strategies strategies like aes progressed encryption standard des information encryption standard and rsa scramble information making it garbled to unauthorized clients without the unscrambling key steganography procedures strategies such as slightest noteworthy bit lsb steganography are utilized to stow away data inside interactive media records like pictures sound and video without causing obvious changes half breed approaches a few frameworks endeavor to progress security by combining cryptographic encryption with steganographic inserting whereas these strategies improve information security they moreover show certain restrictions that foes can abuse impediments of the existing framework 1 defenselessness to cryptanalysis in the event that the cryptographic key is uncovered scrambled information can be effectively unscrambled by assailants compromising touchy data 2 defenselessness to steganalysis propels in machine learning and factual examination make it conceivable to distinguish covered up information in media records particularly when utilizing unsurprising designs 3 unsurprising inserting designs routine LSB procedures regularly implant information successively over pixels making the alterations simpler to distinguish through computerized instruments 4 single-layer security depending on as it were encryption or steganography gives constrained assurance against progressively modern cyber dangers 5 tall computational overhead a few encryption strategies request considerable handling assets making them unacceptable for real-time or resource-constrained situations

PROPOSED SYSTEM

Proposed system to overcome the restrictions of conventional strategies this extend proposes a secure framework that combines aes encryption with consecutive lsb-based steganography the framework scrambles the mystery message employing a user-provided private key and the aes calculation the coming about scrambled message is at that point inserted into the slightest noteworthy bits of the cover image pixels successively the method incorporates the taking after steps 1 aes-based message encryption the mystery message is scrambled utilizing the aes calculation with a private key guaranteeing solid information privacy 2 successive pixel inserting the scrambled information bits are covered up consecutively into the slightest noteworthy bits of the cover picture pixels 3

single-component adjustment information is implanted carefully to influence as it were one color component per pixel minimizing obvious distortion 4 key-based information extraction as it were clients with the proper private key can effectively extricate and unscramble the covered up data focal points of the proposed framework 1 dual-layer security combining aes encryption with steganography gives two solid layers of assurance defending the information indeed in case one layer is compromised 2 resistance to steganalysis in spite of the fact that implanting is consecutive the utilize of aes encryption guarantees that indeed in case covered up information is recognized it remains safely garbled without the key 3 tall information keenness the framework guarantees that as it were clients with the proper decryption key can recover the first message precisely 4 minimal visual affect implanting into the slightest critical bits guarantees that the changes to the cover picture are subtle to the human eye 5 proficient preparing aes encryption combined with basic successive inserting permits for quick real-time secure communication without overwhelming computational requests.

III. MODULE DESCRIPTION

This system has been broken into well-defined components to manage each part of the process individually. Each module is built with a specific purpose in mind, making the system more organized and easier to maintain. Below is a breakdown of each core module and what it handles.

1. AES Module

This part of the system handles the core encryption and decryption logic. It takes the user's secret message and applies the AES (Advanced Encryption Standard) algorithm using a private key provided by the user. The same key is required to reverse the process and retrieve the original text from the encrypted version. The module uses a fixed initialization vector for consistency and employs Java's built-in crypto libraries.

2. Image Encoding Module

This module is responsible for hiding the encrypted data inside an image. It works by altering the image's pixel data — more specifically, the least important bits— to store the hidden message. It only touches one of the color channels per pixel to keep the visual quality of the image intact. The embedding process follows a straight, step-by-step approach through the image to make sure everything fits properly.

3. Image Decoding Module

The decoding part of the system looks through the stego-image and pulls out the bits that were previously hidden. Once those bits are collected and rearranged back into a byte array, the system can decrypt them using the AES module to recover the original message. If the wrong key is used, the system ensures that the output remains unreadable, preserving data security.

4. User Data Handler (AppForm Module)

This module is a simple container that carries the user's input data. It stores things like secret messages, the key, the selected image, and the type of operation the user wants to perform. By using this structure, it becomes easier to pass user data between different parts of the system.

5. File Manager Module

This part of the system keeps track of where files are stored. When users upload an image or when the application saves a new stego-image, this module ensures the files are placed in the correct folder. The path is centralized so that all file operations use the same location, reducing the chance of error.

6. Web Interface (JSP Modules)

These files make up the visual part of the application that users interact with. Pages like encode.jsp and decode.jsp allow users to hide or reveal messages, while login.jsp and registration.jsp manage user access. Each page connects with the backend modules to trigger the required operations based on user actions.

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

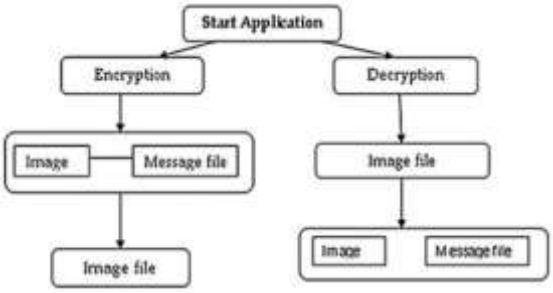

Fig. System Architecture

V. OUTPUT SCREENS

FIG : Home Page

FIG: Registration Page

FIG: Login Page

FIG: Encode Page

FIG: User Uploading Image

FIG: User Input Message

FIG: User 16 Digit Private Key

FIG: Decode Page

FIG: User Uploading Encoded Image

FIG: User Giving Private Key

FIG: Final Output (user retrieving information from image)

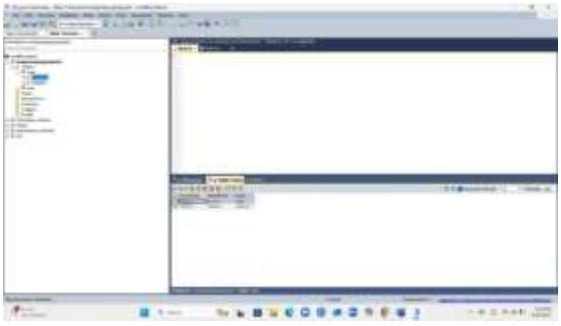

FIG: Database Table

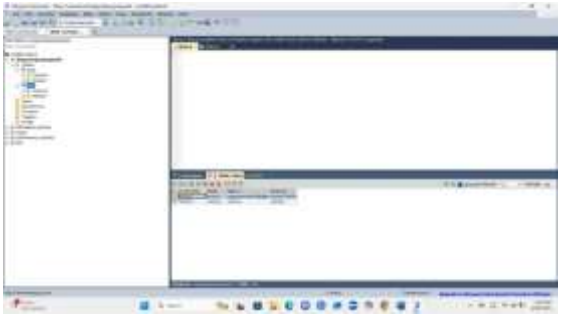

FIG: Database Tables

VI. CONCLUSION

In this research, a steganographic framework was created by combining computerized information stowing away methods with secure message transmission standards. The proposed approach overcomes impediments in existing strategies by utilizing Least Significant Bit (LSB) inserting and particular adjustment of RGB components to conceal mystery messages inside pictures. In spite of the fact that AES encryption usefulness is accessible inside the extend, the current usage implants the crude message without earlier cryptographic encryption to preserve effortlessness and effectiveness. This lightweight plan guarantees tall secrecy whereas keeping the covered up information outwardly imperceptible to assailants. Test comes about illustrated that the framework successfully covers up delicate data without causing unmistakable twists within the cover picture. The created strategy appears solid potential for applications such as secure communication, secret information sharing, online exchanges, and data assurance in cloud situations. Future progressions, counting the integration of AES encryption, versatile steganography strategies, blockchain-based confirmation, and quantum-resistant security models, may advance upgrade the unwavering quality and vigor of this framework.

REFERENCE

1. SREELAKSHMI (2015, NOV 9). “Image steganography using LSB,” https://www.slideshare.net/Sreelekshmi Sree1/image- steganographyusing-lsb (accessed: February 27, 2019).
2. K. Curran and K. Bailey, “An Evaluation of Image Based Steganography Methods,” Multimedia Tools and Applications, Vol. 30 Issue 1, pp. 55 – 88, July 2006.
3. Osuolale and A. Festus, “Secure Data Transfer Over the Internet Using Image Crypto Steganograph y.” in International Journal of Scientific & Engineering Research, 8(12), pp. 6-9,

December 2017.
4. S. Singh and V. K. Attri, “Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm “, in International Journal of Signal Processing, Image Processing and Pattern Recognition,Vol. 8, No. 5, pp. 259- 266, 2015.
5. R. Böhme, “Advanced Statistical Steganalysis information security and cryptography,” in New York, NY: Springer. DOI: 10.1007/978- 3- 642-14313-7, May 2010.
6. K.S. Seethalakshmi, Usha. B, and Sangeetha. K. N, “Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography,” in IEEE Int. Conf. Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016.
7. S. Bukhari, M. S. Arif, M.R. Anjum and S. Dilbar, “Enhancing security of images by Steganography and Cryptography techniques”, in IEEE Int. Conf. Innovative Computing Technology (INTECH), 2016.
8. R. Das, I. Das, “Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques”, in IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN), 2016.
9. A. Gambhir and S. Khara, “Integrating RSA Cryptography & Audio Steganography”, in IEEE ICCCA, 2016.
10. K. Joshi, R. Yadav, “A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication,” in IEEE ICIIP, 2015.
11. V. Shanna and Madhusudan, “Two New Approaches for Image Steganography Using Cryptography” in IEEE Int. Conf. Image Information Processing, 2015.
12. M. Mukhedkar, P. Powar and P. Gaikwad, “Secure non-real- time image encryption algorithm development using cryptography & Steganography”, in IEEEINDICON,2015.
13. R. Indrayani, H. A. Nugroho, R. Hidayat, I. Pratama, “Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function,” in International Conference on Science and TechnologyComputer (ICST), IEEE, 2016.
14. N. Patel, S. Meena, “LSB Based Image Steganography Using Dynamic Key Cryptography”, in International Conference on Emerging Trends in Communication Technologies (ETCT), 2016.