ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

STEGANOGRAPHY TOOL FOR SECURE MESSAGE HIDING WITH AES ENCRYPTION

I.Sai Shriya
21N81A6270
Computer Science and Engineering
(Cyber Security)
Sphoorthy Engineering College,
Nadergul, Hyderabad,501510
Shriyainala19@gmail.com

R.Deepthi
21N81A6266
Computer Science and Engineering
(Cyber Security)
Sphoorthy Engineering College,
Nadergul, Hyderabad,501510
rvamshirvamshi18@gmail.com

B. Arjun
21N81A62A2
Computer Science and Engineering
(Cyber Security)
Sphoorthy Engineering College,
Nadergul, Hyderabad,501510
Boyenpallyvani010@gmail.com

A. Mohan Reddy
21N81A6288
Computer Science and Engineering
(Cyber Security)
Sphoorthy Engineering College,
Nadergul, Hyderabad,501510
sunnyreddy970@gmail.com

Dr.Subbarao.K
Head of the Dept.
Research and Development Sphoorthy Engineering College,
Nadergul, Hyderabad,501510

ABSTRACT:

The primary goal of this project is to create a user-friendly tool that allows us to encode secret text within image files while ensuring minimal distortion to maintain image quality. This project presents a hybrid approach that combines Advanced Encryption Standard (AES) and Least Significant Bit (LSB) image steganography to achieve both

confidentiality and invisibility in message transmission.

The process begins with encrypting a secret message using the AES algorithm, which transforms the message into an unreadable ciphertext using a user-defined password. This encrypted data is then converted into binary format and embedded into the least significant bits of pixel values in a cover image using the LSB technique. A Graphical User Interface (GUI) built with Python's Tkinter library facilitates an intuitive interaction, allowing users to easily encode and decode messages by selecting an image, entering a message and password, and viewing results within seconds.

Keywords— Cybersecurity, Confidentiality,Privacy,Encryption.

INTRODUCTION

In today's digital age, where data breaches and unauthorized access are on the rise, confidentiality and secrecy during communication are the need of the hour. This project provides a secure method of hiding sensitive data in images using the Least Significant Bit (LSB) steganography technique in addition to Advanced Encryption Standard (AES) encryption.

The method encrypts the user's secret message first with AES, making it unintelligible in the form of ciphertext. The encrypted message is subsequently hidden in the least significant bits of the pixels of an image, resulting in a stego image that is indistinguishable from the original image. The outcome is a two- layered security system: even if the concealed data is found, it is still concealed behind robust encryption.

On the receiving side, the system reads out the hidden ciphertext from the image and decrypts it using the correct AES password to get the original message. A graphical user interface (GUI) is used for an easy-to-use process, thus making it simple to enter messages, manage passwords, and select images.

LITERATURE REVIEW

1.A Secure Image Steganography Based on RSA Algorithm and Hash-LSB technique Overview: Integrates RSA encryption and Hash-LSB steganography for enhanced security.
Methodology: RSA encrypts the message before embedding using LSB with hashed pixel selection.
Source: IEEE Xplore, 2017.
Drawbacks: RSA is slower compared to symmetric encryption and increases message size.

2.A Modified LSB Technique of Digital Image Steganography Using Genetic Algorithm

Overview:Optimizes LSB embedding using Genetic Algorithms to reduce distortion.
Methodology: Genetic algorithms identify optimal pixels to embed data with minimal perceptual change.
Source: ScienceDirect, 2018.
Drawbacks: High computation time and complexity; difficult to implement in real-time systems.

3.Steganography and Cryptography Techniques:

Overview: Reviews various techniques, highlighting benefits of combining encryption with steganography.
Methodology: Comparative analysis of AES, DES, RSA with LSB, DCT, and DWT steganography methods
Source: Springer, 2019.
Drawbacks: High-level review; lacks implementation or real-time validation.

METHODOLOGY

The **LSB technique** is one of the simplest and most widely used methods in image steganography. It works by replacing the **least significant bits** of image pixel values with the bits of the secret message (e.g., text, file, etc.). Since changes to LSBs have minimal impact on the overall pixel value, the visual quality of the image remains nearly unchanged.
Example:
Original pixel RGB value:
R = 100 (01100100)
Message bit to embed: 1
New R value: 101 (01100101)← LSB changed from 0to 1

PROPOSED SYSTEM

The proposed system enhances traditional LSB steganography by integrating it with strong cryptographic techniques like **AES (Advanced Encryption Standard)** or **RSA (Rivest–Shamir–Adleman)**, coupled with **hashing mechanisms** or **optimization algorithms** such as the **Genetic Algorithm (GA)**. This two-layered approach ensures both **security** and **imperceptibility**.
In this system:
The **secret message is first encrypted** using AES or RSA to make it unreadable without the proper key.The **encrypted message is then embedded** into the image using a **randomized or optimized LSB embedding** technique, which strategically selects pixels to hide the data based on a hashing function or an optimization algorithm.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

Advantages of the Proposed System

Enhanced Security

– Encryption ensures that even if the embedded data is detected or extracted, it remains indecipherable without the decryption key.

Improved Stealth

– Randomized or optimized pixel selection breaks predictable patterns, making the hidden data less detectable by steganalysis tools.

Data Confidentiality

– The dual-layered security of encryption followed by steganography ensures that the message remains private and secure.

Better Image Quality

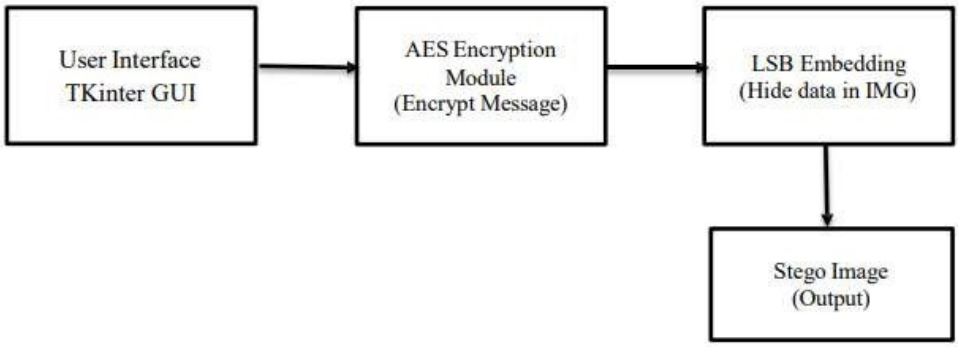
– Optimization techniques like Genetic Algorithms reduce the visual impact of embedding, maintaining high perceptual quality of the cover image.

Resilience to Attacks

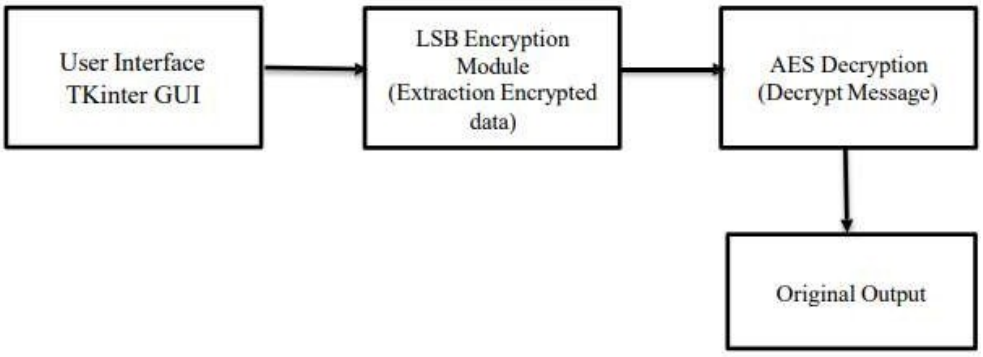
– The combined approach increases resistance to image processing operations such as compression, resizing, filtering, and noise addition.

SYSTEM ARCHITECTURE

ENCODING



DECODING



INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

RESULT ANALYSIS

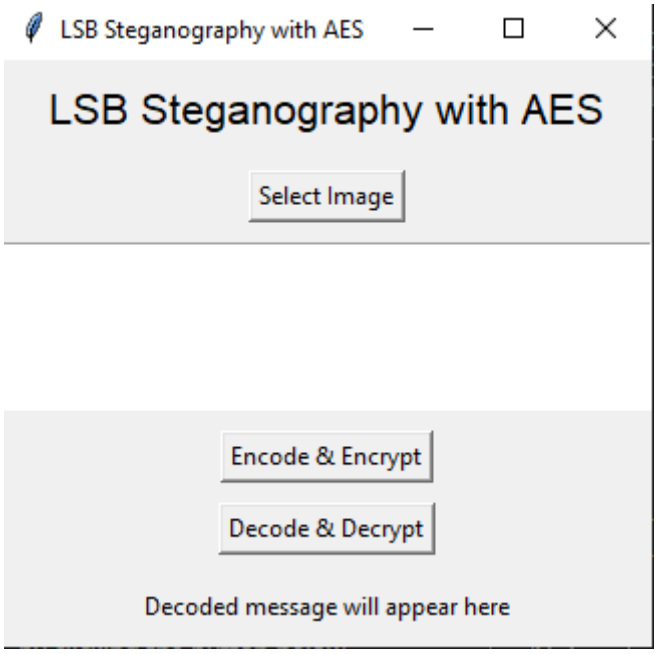


Fig 1: GUI for Tool

```
[Step 1] Binary message:
01001000011001010110110001101100011011111

[Step 2] Embedding message bits into image:

Pixel (0,0) RED: 43 -> 42 (bit: 0)
Pixel (0,0) GREEN: 12 -> 13 (bit: 1)
Pixel (0,0) BLUE: 0 -> 0 (bit: 0)
Pixel (1,0) RED: 88 -> 88 (bit: 0)
Pixel (1,0) GREEN: 56 -> 57 (bit: 1)
Pixel (1,0) BLUE: 33 -> 32 (bit: 0)
Pixel (2,0) RED: 96 -> 96 (bit: 0)
Pixel (2,0) GREEN: 62 -> 62 (bit: 0)
Pixel (2,0) BLUE: 34 -> 34 (bit: 0)
Pixel (3,0) RED: 93 -> 93 (bit: 1)
Pixel (3,0) GREEN: 57 -> 57 (bit: 1)
Pixel (3,0) BLUE: 23 -> 22 (bit: 0)
Pixel (4,0) RED: 98 -> 98 (bit: 0)
Pixel (4,0) GREEN: 60 -> 61 (bit: 1)
Pixel (4,0) BLUE: 23 -> 22 (bit: 0)
Pixel (5,0) RED: 96 -> 97 (bit: 1)
Pixel (5,0) GREEN: 57 -> 56 (bit: 0)
Pixel (5,0) BLUE: 18 -> 19 (bit: 1)
Pixel (6,0) RED: 99 -> 99 (bit: 1)
...
Pixel (18,0) RED: 36 -> 37 (bit: 1)
Pixel (18,0) GREEN: 34 -> 34 (bit: 0)

 Message encoded and image saved as: C:\Users\DELL\OneDrive\Pictures\Pic1_encoded.png
```

Fig 2: Encrytion of bits

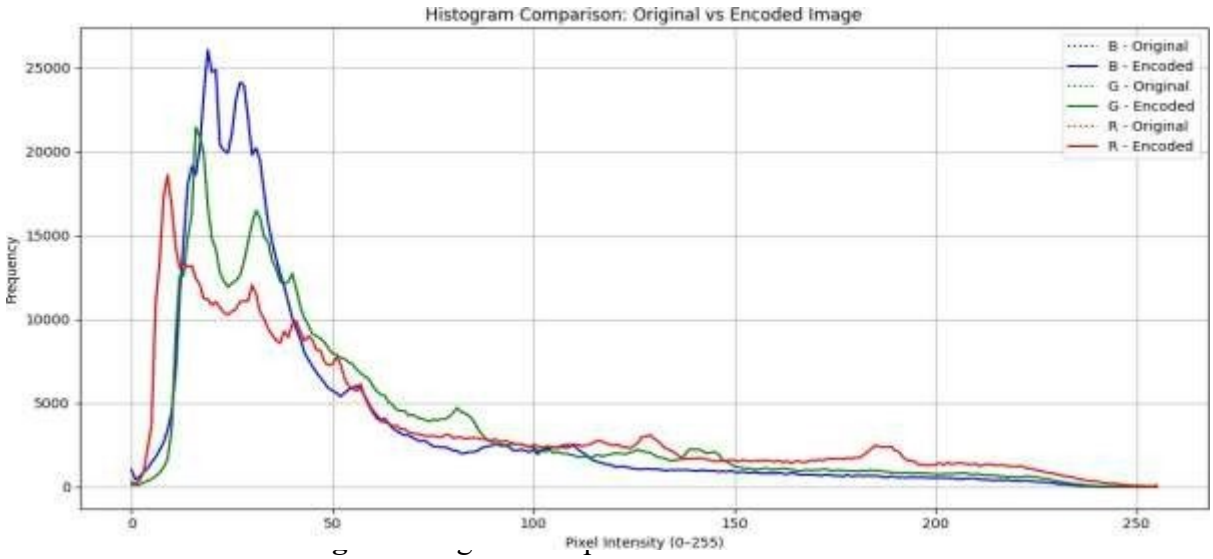
INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

```
[Step 1] Extracting LSBs from pixels:

Pixel (0,0) RED LSB: 0
Pixel (0,0) GREEN LSB: 1
Pixel (0,0) BLUE LSB: 0
Pixel (1,0) RED LSB: 0
Pixel (1,0) GREEN LSB: 1
Pixel (1,0) BLUE LSB: 0
Pixel (2,0) RED LSB: 0
Pixel (2,0) GREEN LSB: 0
Pixel (2,0) BLUE LSB: 0
Pixel (3,0) RED LSB: 1
Pixel (3,0) GREEN LSB: 1
Pixel (3,0) BLUE LSB: 0
Pixel (4,0) RED LSB: 0
Pixel (4,0) GREEN LSB: 1
Pixel (4,0) BLUE LSB: 0
Pixel (5,0) RED LSB: 1
Pixel (5,0) GREEN LSB: 0
Pixel (5,0) BLUE LSB: 1
Pixel (6,0) RED LSB: 1
Pixel (6,0) GREEN LSB: 0
Pixel (6,0) BLUE LSB: 1
Pixel (7,0) RED LSB: 1
...
 010010000110010101101100011011000110111l

 Decoded Message:
 Hello
```

Fig 3: Decryption of bits



CONCLUSION

In conclusion, the project "Secure Image-based Communication using LSB Steganography and AES Encryption" successfully demonstrates the integration of cryptographic and steganographic techniques to ensure both confidentiality and concealment of sensitive information. By combining the Advanced Encryption Standard (AES) with the Least Significant Bit (LSB) method, the system provides a robust two-layer security approach — encryption protects the content, while steganography hides its presence.

The developed Python-based tool features a user-friendly graphical interface (GUI) that enables non-technical users to easily encode and decode secret messages. The tool allows users to input their own passwords, making encryption dynamic and more secure. The system ensures minimal distortion to the image, maintaining its visual integrity while successfully embedding encrypted data.

Extensive testing, including unit, integration, and performance testing, confirms the reliability and efficiency of the tool. The implementation offers a practical solution for secure communication over untrusted networks, with possible applications in fields such as digital forensics, private messaging, and secure watermarking.
Overall, this project bridges the gap between data security and data concealment, showcasing the effectiveness of hybrid security approaches in modern digital communication.

FUTURE SCOPE

The project can also include other variants of Steganography like Audio ,Video , Files.etc., to complete the tool. As Cybercriminals increases day by day, some features may be included or replaced with new ones to escape them.

REFERENCES

[1]S. K. Bandyopadhyay and A. Das,
"A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", IEEE Xplore, 2017.
https://ieeexplore.ieee.org/document/8010663
[2]R. Chandramouli, N. Memon,
"Analysis of LSB-Based Image Steganography Techniques", Proceedings of the IEEE, 2001.
https://ieeexplore.ieee.org/document/929893
[3]P. G. Chavan, S. S. Patil,

"Combination of AES and Steganography for Secure Data Communication", IJSRSET, Vol. 6, Issue 3, 2020.
https://ijsrset.com/IJSRSET203851
[4]M. S. Bhatnagar, S. Khurana,
"Secure Image Steganography Using AES and LSB Substitution", International Journal of Computer Applications, Vol. 174, No. 3, 2021. https://www.ijcaonline.org/archives/volume174/number3/
[5]N. Provos and P. Honeyman,
"Hide and Seek: An Introduction to Steganography", IEEE Security & Privacy, Vol. 1, No. 3, 2003. https://ieeexplore.ieee.org/document/1203220