The Scientific Temper (2025) Vol. 16 (2): 3803-3811
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2025.16.2.12
https://scientifictemper.com/

RESEARCH ARTICLE

A secure messaging application using steganography and aes encryption: A dual-layer secure messaging system

S. Gomathi*, C. Radhika

Abstract

This research involves the development of a secure messaging application with the capability to send messages inside images of or audio files using the practice called steganography. In this application, a person can secretly communicate in such a way that no one is aware of the existence of the hidden message. The application uses the least significant bit (LSB) method to hide the messages while encrypting the messages. To provide greater security, AES encryption is used before hiding the messages, thus forcing both sender and receiver to decrypt the message using a shared key. This two-layer approach of steganography and encryption makes this application highly appropriate for people with communication controls or monitored at some level because it gives confidentiality for message privacy.

Keywords: Steganography, Secure messaging, Data hiding, LSB method, AES encryption, Privacy, Hidden communication.

Introduction

In the modern digital world, personal and sensitive information is often spread through the internet. Ensuring private communication is safe is a crucial aspect of encryption, which ensures strong data security by transforming plaintext into unreadable formats; however, it arouses suspicion quite often, since its existence points to the protection of important or sensitive information. The process of steganography entails hiding messages within seemingly innocuous media, such as pictures, sounds, or videos. This conceals the presence of the message to potential observers. This paper combines the benefits of steganography with encryption in order to build a secure messaging tool that will ensure anonymity and confidentiality. The application utilizes the least significant bit (LSB) technique, a widely used method in steganography that integrates encrypted information into the least significant bits of image pixels or audio sample values. This approach is exceptionally effective as it introduces negligible visual or audio distortion, rendering the hidden message undetectable to human perception. In terms of security, the application encrypts the message using the AES technique before hiding. AES is a secure, fast symmetric encryption method known for excellent security with great speed in performance and highly applied in numerous applications. It makes the application ensure that the discovered hidden message remains unreadable if it were found without an appropriate decryption key (Donald L. Evans *et al*., 2023).

This dual-layered security system grants an unprecedented level of security by concealing and protecting information, thereby conclusively decreasing threats through illicit access and discovery. This strategy is very useful where privacy is critical such as whistle-blowers, corporate data exchange, military communication, or scenarios with oppressive surveillance. With that, users without a technical background can easily use the application because it has integrated intuitive features that can be used along with these advanced security procedures. This project underscores the importance of innovation in digital security and sets a new benchmark for discreet and dependable communication in a rapidly changing technical environment.

Image Steganography

The rapid advancement of imaging technologies and devices has led to the production of high-resolution and accurate

Shrimathi Devkunvar Nanalal Bhatt Vaishnav College for Women, Chrompet, University of Madras, Chennai, Tamil Nadu, India.

***Corresponding Author:** S. Gomathi, Shrimathi Devkunvar Nanalal Bhatt Vaishnav College for Women, Chrompet, University of Madras, Chennai, Tamil Nadu, India, E-Mail: gomathi.s@sdnbvc.edu.in

How to cite this article: Gomathi, S., Radhika, C. (2025). A secure messaging application using steganography and aes encryption: A dual-layer secure messaging system. The Scientific Temper, **16**(2):3803-3811.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.2.12

Source of support: Nil

Conflict of interest: None.

Received: 28/12/2025 **Accepted:** 11/02/2025 **Published** : 20/03/2025

images. Additionally, the rapid expansion of the internet has facilitated the transfer of vast quantities of information, including these images, much of which requires secure and private transmission. Consequently, steganography assumes a function in the domain of information security (Zaid Al-Omari *et al*., 2015).

Although virtually any kind of file can be utilized in digital image steganography, the great degree of redundancy in images makes them the most ideal for embedding (Tayana Morkel *et al*., 2005). Three factors are essential for this study to investigate or develop image steganography systems (Namrata Singh 2017): commonly termed as the payload, capacity denotes the maximum quantity of data that a cover image can contain. The image's durability against various compression and processing methods. Invisibility, Security, or imperceptibility: minimizing alterations to the cover image to enhance the resilience of the resultant stego image against steganalysis and the human visual system (HVS). This study uses the least significant bit (LSB) encryption technology to conceal messages. Prior to message concealment, AES encryption is used to increase security. This forces the sender and receiver to utilize a shared key to decrypt the message.

1. Least Significant Bit (LSB)

In LSB substitution dominates spatial domain steganography. It changes the image's least significant piece of pixel values. The least significant bit has little effect on pixel color, therefore replacing it with the disguised message does not change the image (Indu Nehra *et al.* 2015).

- *Mechanism of operation:*
  - Convert the sensitive text, binary data, or image to binary.
  - Determine carrier image pixel values.
  - Replace the least significant bit of each color channel (Red, Green, Blue) In each pixel with the hidden message.
  - Since the bit substitution is small,the altered image will look almost identical to the original.
- *Illustration:*
  - RGB original pixels:210 |173 | 241.
  - Binary confidential communication: 01001000 (H).
  - Replace the least important red, green, and blue bits:
  - Red:11010010→11010000;
    Green:10101101→10101100
  - Blue: 11110001 →11110000

2. Advanced Encryption Standard (AES):

In steganography, AES encrypts a confidential message prior to concealing it within a carrier, such as an image, audio, or video file (Ako Muhamad Abdullah *et al*., 2017).

- *Mechanism of operation:*
  - Utilize AES for message encryption.
  - Incorporate Encrypted Communication: Conceal the encrypted message within the carrier media (e.g., least significant bits of an image).
  - Extract and Decrypt: The recipient retrieves the concealed data and decrypts it with the AES key to obtain the original message.
  - AES guarantees that even if concealed data is uncovered, it remains protected by encryption.

Objectives

The main goal of this project is to create a secure messaging app that hides messages in image files using steganography. The app will use the least significant bit (LSB) method to conceal messages so that they remain undetected. To ensure security, hidden messages will be encrypted, making them unreadable without the right key. The app will have an easy-to-use interface for inputting messages and uploading media. It will also support real-time messaging for seamless communication.

Related Works

A safe and reliable method for protecting sensitive data was suggested in a study by (Mamta Juneja *et al*., 2013). A two-part least significant bit (LSB) technique for encoding secret information is presented in the paper. Using this technique, data is partially embedded into the green components and the LSBs of randomly chosen pixel locations along the margins of images. Present also is an adaptive LSB-based steganography method that, in smooth regions of the picture, inserts data depending on the information accessible in the MSBs of the RGB components of randomly selected pixels. Adding support for the advanced encryption standard (AES) strengthens this method. A novel LSB-based data embedding method is presented by S. Shanmuga Priya *et al*. (2012). This method treats a pair of pixels as a single unit, encoding one bit in the LSB of the first pixel and another in a function of the two-pixel values. This procedure improves distortion reduction and steganalysis resistance. Data embedding is performed to sharper edge regions with a threshold. PSNR values are also examined for adaptive and nonadaptive data-hiding strategies in grayscale and color images. Jeba Nega Cheltha C *et al*. (2021) discussed cryptography and steganography techniques for protecting data transfer. The paper demonstrates how different techniques may enhance the security of communication together. AES, steganography, and other cryptographic techniques are discussed to embed encrypted data in images and audio files. Cryptography and steganography offer a multi-layered security solution that keeps a message indecipherable without the decryption key. In addition, (Vishwakarma Singh *et al*., 2023) proposed a secure

messaging application using AES encryption for Android devices. This research focuses on the use of AES to ensure message confidentiality and integrity, thus preventing unauthorized access to communications. The combination of AES encryption with steganography may enhance the security of this communication system by hiding the encrypted message in an image or audio file.

(Guobin Hao *et al*., 2023) proposed a secure image steganography communication system for unmanned aerial vehicles (UAVs) in the realm of real-time communication. Their technology integrates encrypted data within

Photographs, subsequently sent between UAVs to securely provide navigation and positioning information. The implementation of AES encryption in conjunction with steganography guarantees the confidentiality and security of essential data, even within a collaborative, dispersed setting. In (Ilyas Yaqoob, 2018), examine diverse encryption and decryption methodologies, emphasizing the energy consumption effects of algorithms like DES and AES. The authors evaluate AES-256 with alternative algorithms, concluding that AES-256 provides superior security and reduced power consumption, hence enhancing battery longevity on mobile devices. The document emphasizes the advantages of AES-256 in decreasing encryption and decryption durations, hence improving device performance without sacrificing security. (Ritu Sindhu *et al*., 2020) provide the review of numerous steganography approaches, methods, standards, advantages, disadvantages, and sample files, a few of them that do not require bitmap conversion and those memory-optimized ones. (Rizky Riyaldhi *et al*., 2017), This paper introduces a new optimization method for the AES algorithm by modifying the Shift Row and S.Box methods for Mix Column transformation. This optimization has reduced processing time by 3 ms and is still improving within creased byte counts. The average percentage of optimization is 86.143%. (Sistla Vasundhara Devi *et al*., 2019), The principal advantage of AES is its ability to be implemented or operated with pure hardware. In this paper, Xilinx9.2i has been used for the simulation and

Optimization of VHDL code. The implementation and simulation of code were done using the Xilinx Project Navigator ISE 9.2i. The Xilinx XC3S500 is a member of the Spartan Family and is used as the device for hardware designs. This plan aims at synchronizing the AES encrypter with the AES decryption (Nandhini Subramanian *et al*., 2021), The main focus of this research is to observe and analyze various deep learning techniques used in the image steganography field.

Deep learning techniques used for image steganography can be divided into three: classic methods, CNN-based methods, and GAN-based methods. This paper gives an overview of the datasets used, the experimental configurations explored, and the commonly used evaluation metrics along with the approach. (Handrizal *et al*., 2021), Steganography using modified least significant bit, columnar transposition cipher, Caesar cipher, and multiplication with carry generator for picture embedding succeeds well. Larger messages take longer to embed. A 10x10 message covering 1000 takes 30.9182 ms to embed, while an 80x80 message spanning 3000 takes 85555.1237 ms. Time extraction depends on message size; it takes more time for larger messages. A 10x10 message covering 1000 takes 33.9084 ms to extract whereas an 80x80 message covering 3000 takes 87321.2564 ms. MSE and PSNR depend on the message and cover object dimensions. The lower embedded message size and higher size of the cover object improve the MSE and PSNR. In (Prasann Parikh *et al*., 2024), described four fundamental cryptography techniques. The Data Encryption

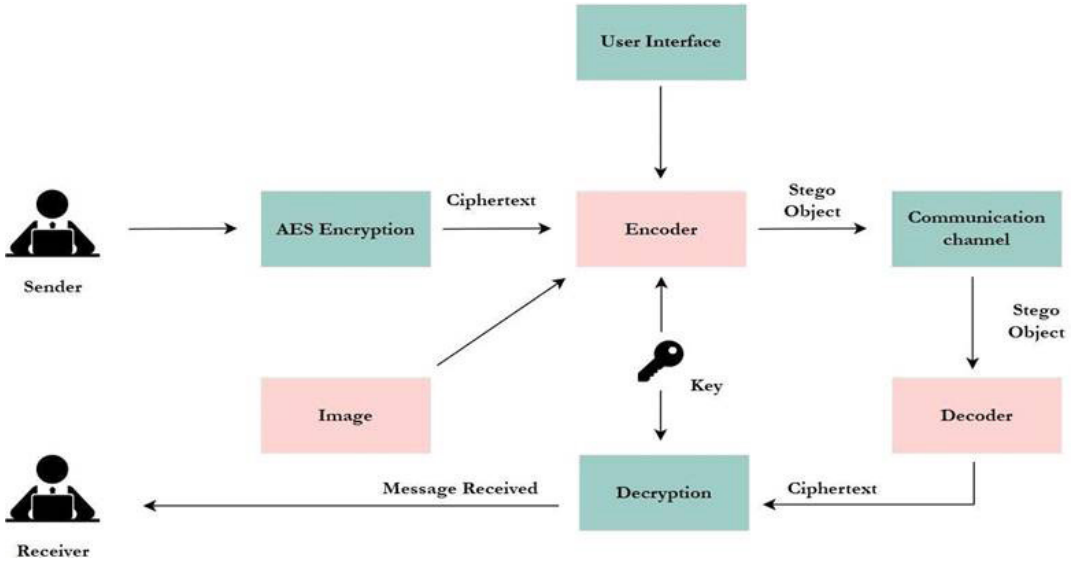

Figure 1: Architecture diagram

Standard (DES), a symmetric-key encryption, is examined for its susceptibility to brute-force attacks. The advanced encryption standard (AES) is a more secure alternative that utilizes 128-bit blocks and supports key sizes of 128, 192, and 256 bits. The document analyzes Rivest–Shamir–Adleman (RSA), an asymmetric encryption technique that employs a public and private key pair for secure communication.

Proposed Methodology

The steganography-based message application model details a secure process for embedding and extracting encrypted messages within image files. Here's how the system operates: Figure 1: Illustrates an overview of a proposed methodology architecture diagram.The methodology in question has turned out to be interesting and strong as it combines both steganography and encryption such that any message hidden within the media files, either images or audio, remains secure making it quite easy to have an isolated communication system. The steps are detailed as follows:

Message Input

Through the application's interface user-initiated message input where the user can input a text message directed to the recipient.

Encryption

A text message has been issued with a user message encryption whenever the sender uses an AES algorithm. In this encryption step, even if the secret message is found, it is kept confidential to everyone who does not have the correct key.

Steganographic Embedding

Using the LSB technique, the hidden text of the message is first inserted into the integer image. Although it is intended to be imperceptible, this technique mathematically alters the last eighth bit in a byte of a number representing a particular pixel of an image (or sample of sound), with little visible distortions brought about by the insertion of bits. This modification has an encrypted message embedded in it.

Transmission

The media data which has been altered in the course of embedding the hidden information which in this case was the message is then sent over to the intended recipient through the backend server in a safe socket-controlled channel system.

Extraction and Decryption

After the message has been received, the media file is sent to the applicant's program and the hidden text is opened allowing the embedded information to be retrieved.

Security Analysis

This implies that even if a hidden message is found, it will not be understood without the decryption key. AES encryption secures the hidden message. It is evident that the combined application of LSB steganography and encryption together provides a high-security level for sensitive messages.

Algorithm of Proposed Methodology

The backend algorithm is

3. Encrypt and Encode.

- Step 1: Accept Input: Receive frontend messages and photos, Verify message and image input. Noncompliance generates an error.
- Step 2: Generate AES Key: Use get_aes_key to generate a 32-byte AES key from a string, Use a random Initialization Vector to encrypt the message using AES in CFB mode.
- Step 3: Code encrypted message: Encode the encrypted message and initialization vector (IV) in Base64.
- Step 4:LSB Steganography hides the base64-encoded encrypted message in the image, keep encoded image: Keep the altered image with the secret message.
- Step5:Update the frontend with the encoded image as a download, Hidden hidden message in the encoded image.

4. Decrypt

- Step1:Accept Input: Frontend-encoded picture, Authenticate Input: Check image transmission. Return an error otherwise.
- Step2:Expose Secret Communication: Extract the encrypted message from the image using LSB Steganography.
- Step3:decode Use the AES key to decrypt the encrypted message and retrieve the original message.
- Step4:Decrypted Message:Reply with the decrypted message. Step5: Got the deciphered message.

Frontend Development Algorithm

5. Encode message and image

- Step 1: To verify input, ensure that the message and image are provided. Otherwise, notify of the error.
- Step 2: Generate Random Key: Generate a random encryption key. Step3:Use the produced random key to encrypt the message with AES.
- Step4:Compile Form Data: Instantiate a Form Data object to send the encrypted message and image to the backend via /encode.
- Step5:Send a POST request to Flask /encode using FormData.
- Step6:Get Encoded Image: After a successful response, retrieve the encoded image from the backend and give the user a URL to download it.
- Step 7:Record the time to encrypt and display the message.
- Step 8: A URL to download the encoded image is provided.

6. Decode message and image.

- Step 1: To Verify Input: Provide image and key. Otherwise, notify of the error.
- Step 2: Verify that the decryption key matches the encryption key.
- Step 3:Create a form data object to send the encoded image to the backend at /decode. POST to Flask /decode using FormData.
- Step 4: After retrieving the message, decrypt it with the key. Decrypt the message using AES.
- Step 5: Display the decrypted message or an error message if unsuccessful.
- Step6:Record how long it takes to understand and present the message. Step 7: The user sees the encrypted message.

Evaluation Metrics

Metrics for evaluating image steganography for the proposed methodology are Payload capacity, MSE and PSNR.

Payload Capacity

The payload capacity of a cover picture measures the amount of data. This statistic holds great importance in steganographic systems, as transmission overhead is directly related to the maximal payload capacity. A metric for it is bits per pixel (Stuti Goel *et al*., 2013).

BPP= Hidden bits/Pixels

Mean Square Error (MSE)

The average of the squared pixel-by-pixel variations between the original and stego-images. It evaluates the data embedding-induced cover image error (Idakwo M.A., *et al*.,2020).

$$\mathrm{MSE} = \left(m^{*}n\right)^{-1} \sum_{i=1} m \sum_{i=1} nI \left[\left(I\left(i,j\right) - k\left(I,j\right)\right]^{2} \text{ - (1)}$$

Allow MSE indicates a good embedding. Image dimensions m, n

I=OriginalImage K=stego-image

Peak Signal to Noise Ratio (PSNR)

PSNR is a common metric for measuring embedding-induced cover picture distortion. This is the ratio of a signal's maximum potential to its distortion noise power. We measure it in decibels. High PSNR indicates high-quality embedding [20].

$$PSNR = 10\mathrm{LOG}\left(\frac{MAX^{2}}{MSE}\right) \text{ - (2)}$$

Results and Discussions

The proposed methodology based on steganography and encryption applied to ensure the safe embedding and extraction of the messages appears very promising regarding both security and performance. This section is going to analyze the effectiveness of combined techniques with regard to performance metrics that lead toward acquiring safe and efficient message transmission. Figure 2 shows the original and the corresponding encoded images of the proposed methodology.

From Table 1 we find that the size of encoded images in PNG is always larger than that of JPEG original images. For instance, Image 1 of size 423x283 was increased to 169 KB in PNG, but it has only 30.3 KB in JPEG format. However, overall embedding results do not deteriorate the image quality significantly so that the technique proves to be successful. MSE is the measure of the difference between the original image and the stego-image. The lower the MSE value, the less distortion is introduced by the data embedding process. For example, in Image 1, the MSE value is 0.5983, which is a relatively low error between the original and encoded images. This shows that the method can hide data with minimal perceptible distortion. As Figure 3 confirms the size for an image representing a normal scenario in Figure 4.

Figure 5 illustrates the increase in image size for Figure 6, which represents the encoded image. The size of the image increases after encoding due to the embedded text. In comparison to other common steganographic techniques, the proposed methodology using LSB with AES encryption introduces less noticeable distortion while maintaining high payload capacity, as indicated by the low MSE values

Table 1: Overview of different metrics used for proposed methodology

IMAGES	*DIMENSION*	*ORIGINAL IMAGE SIZE-JPEG (KB)*	*ENCODE SIZE - PNG(KB)*	*PSNR(db)*	*MSE*	*ENCODE TIME(Sec)*	*DECODE TIME(Sec)*
IMAGE1	423*283	30.3	169	50.36	0.5983	0.685	0.082
IMAGE2	451*373	55.2	285	50.99	0.5181	0.484	0.114
IMAGE3	451*301	51.8	248	50.05	0.6432	0.461	0.091
IMAGE4	500*534	69.0	389	51.23	0.4900	0.602	0.104
IMAGE5	736*488	97.3	735	50.80	0.5415	0.616	0.118

Figure 2: Implementation of original and encoded images.

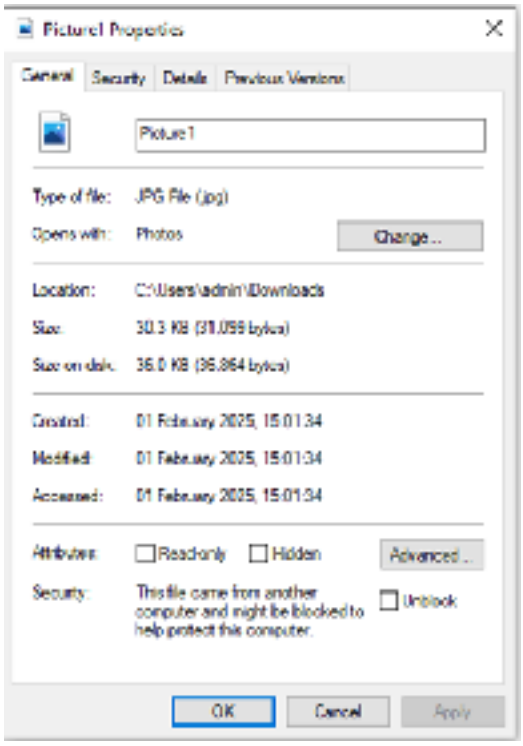

Figure 3: Properties of normal image

Figure 4: Normal image

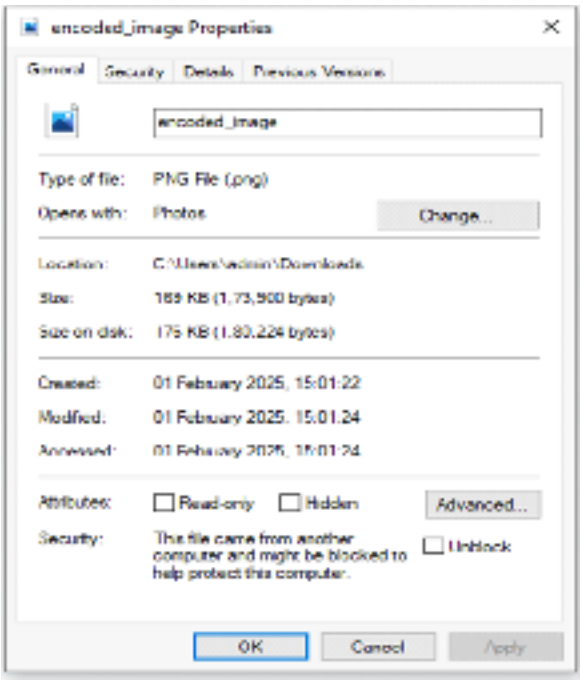

Figure 5: Properties of encoded image

Figure 6: Encoded image

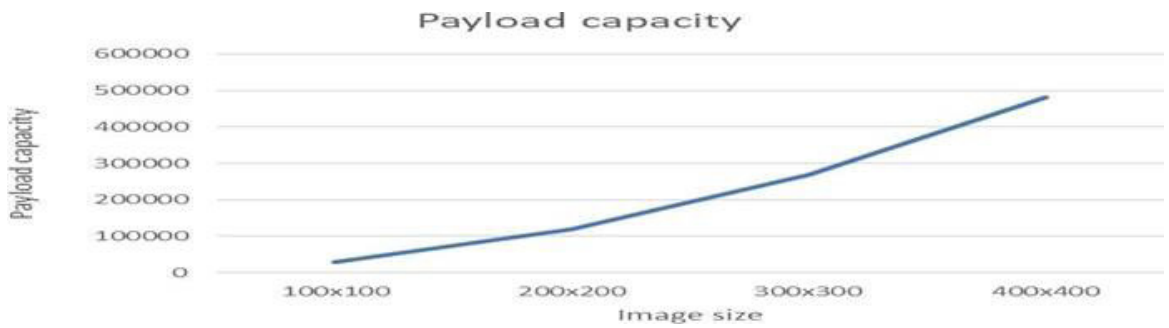

Figure 7: Payload capacity

across the different images ranging from 0.4900 to 0.6432. PSNR is a key indicator of image quality post-embedding, with higher values representing better preservation of the original image. The PSNR values for all encoded images are far above 50 dB and excellent for steganography purposes. For example, Image1 had a PSNR value of 50.36 dB, which meant the encoded image would have been almost indistinguishable from the original with little to no decrease in quality.PSNRs ranging between 50.05 to 51.23 dB for all images indicate that this technique has of negligible visual effect on the quality of the images, making it appropriate for applications where image quality should not be degraded such as in security-sensitive communications. Figure 7 describes the amount of data embedded and the perceptibility of the distortion introduced in the images.

The system's actual efficiency for encoding and decoding times is thus reliant on the following considerations: The proposed system demonstrates reasonable performance with respect to both time metrics, even as the size of the image increases. For instance, in Figures 8 and 9, the encoding time is 0.685 seconds, and the decoding time is 0.082 seconds of the image

These are within the acceptable limits for real-time usage; thus users shall be able to encode and decode messages within very short times while remaining secure. Decoding time remains more or less constant for all the images and is in the range of 0.082 to 0.118 seconds while encoding time increases slightly with larger image sizes. The added security benefits due to the combination of AES encryption with LSB steganography justify the trade-off with respect to speed. Robust security is one of the primary advantages offered by this methodology, as AES encryption and LSB steganography are combined together. Even if the encoded image gets intercepted, the embedded message cannot be extracted because it is encrypted, and decryption will only be possible using the proper decryption key.

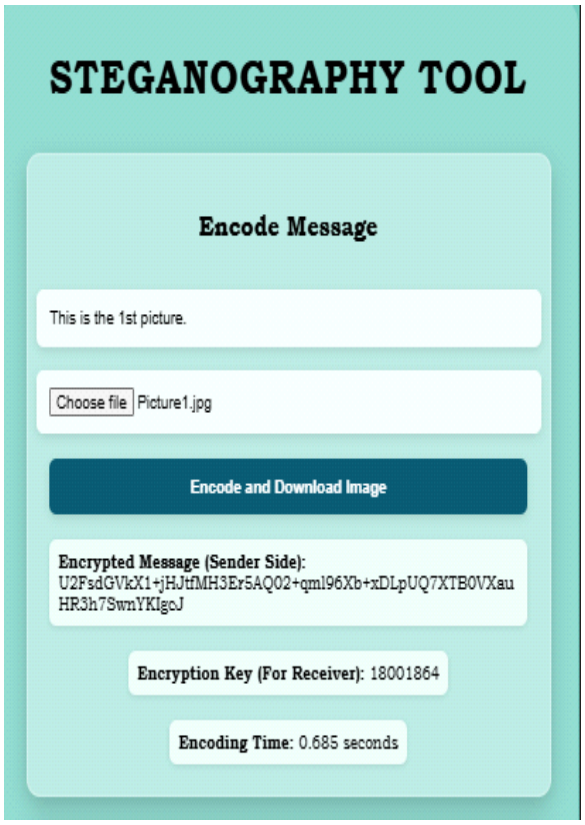

Figure 8: Sender side

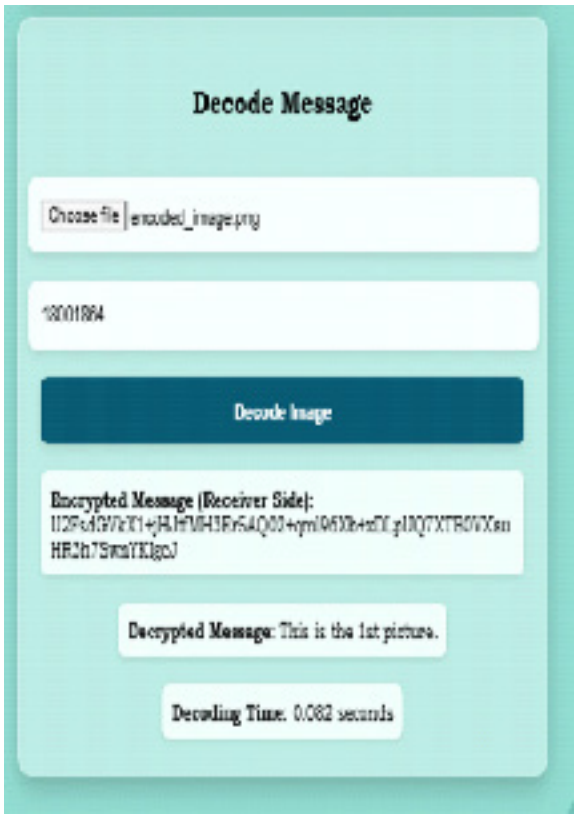

Figure 9: Receiver side

In the case of AES encryption, even if the image is tampered with or analyzed, contents of the message cannot be easily extracted and accessed.

The LSB steganography conceals the encrypted message in such a way that it is not easily detectable, especially in uncompressed formats like PNG, as reflected by the low MSE and high PSNR values.This means that the system provides a high level of security while maintaining message integrity and image quality. When compared to other steganographic techniques, the proposed methodology using LSB steganography combined with AES

encryption offers a better balance of payload capacity, image quality, and security.The system's use of AES encryption ensures that even if the stego-image is intercepted, the hidden message remains secure.In addition, there is minimal perceivable distortion applied to the picture,as in the PSNR and MSE metrics, making the approach more superior than simpler only LSB-based ones.

Conclusion

The application of steganography that integrates AES encryption with LSB-based steganography offers a secure and efficient approach for embedding and extracting messages in images. The findings show that the system attains elevated security, negligible distortion, and satisfactory performance in terms of encoding and decoding times. The analysis shows that this method can be efficiently used for secure communications in applications where message secrecy and image quality are significant. The provided enhancements can then focus on improving the encoding and decoding processes for better speed or researching other image formats that may offer better steganographic capabilities.

Acknowledgment

We, the researchers, acknowledge the below-mentioned authors and their references which were used in preparing the research paper.

References

Ako Muhamad Abdullah, (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. Cryptography and Network Security.

Donald L. Evans, et al.,(2023). Advanced Encryption Standard (AES). Information Technology Laboratory National Institute of Standards and Technology Gaithersburg. MD 20899-8900, https://doi.org/10.6028/NIST.FIPS.197.

Guobin Hao, Guobin Fu. (2023). Research on Image Steganography for the Instant Messaging and Broadcasting in a Collaborative Unmanned Cluster. College of Information and Communication, National University of Defense Technology, Wuhan, China. DOI:10.1109/icctit60726.2023.10436020.

Handrizal et al (2021). Implementation of Steganography Modified Least Significant Bit using the Columnar Transposition Cipher

and Caesar Cipher Algorithm in Image Insertion. Journal of Physics: Conference Series 1898, 012003, doi:10.1088/1742-6596/1898/1/012003.

Idakwo M.A., et al.,(2020). An Extensive Survey of Digital Image Steganography: State of the Art. Journal of Science Technology and Education, ISSN: 2277-0011.

Ilyas Yaqoob, Talha Naqash, Sajjad Hussain Shah (2018). Encryption and Decryption of Mobile Security Using AES and GOST Algorithms. 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON).

Indu Nehra et al (2015). Review Paper On Image Based Steganography. International Journal of Scientific & Engineering Research, 6(6), ISSN 2229-5518.

Jeba Nega Cheltha C, Manik Rakhra, Rajan Kumar, Himdweep Walia(2021). A Review on Data hiding using Steganography and Cryptography. 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).

Mamta Juneja, Parvinder Sing Sandhu (2013). A New Approach For Information Security Using An Improved Steganography Technique. Journal of Info. Pro.System, 9(3), 405-424.

Nandhini Subramanian et.al (2021).Image Steganography: A Review of the Recent Advances. IEEE Access, 99, DOI:10.1109/ACCESS.2021.3053998.

Namrata Singh (2017). Survey Paper on Steganography. International Refereed Journal of Engineering and Science(IRJES), 6(1), 68-71.

Prasann Parikh, Nishil Patel, Dev Patel, Pratham Modi, HargeetKaur(2024). Ciphering the Modern World: A Comprehensive Analysis of DES, AES, RSA and DHKE. 11th International Conference on Computing for Sustainable Global Development.

Ritu Sindhu, Pragati Singh (2020). Information Hiding using Steganography. International Journal of Engineering and Advanced Technology (IJEAT), 9(4), DOI: 10.35940/ijeat.D8760.049420.

Rizky Riyaldhi,Rojali, Aditya Kurniawan (2017). Improvement of Advanced Encryption Standard Algorithm with Shift Row and S.Box Modification Mapping in Mix Column. Procedia Computer Science, 116, 401-407. https://doi.org/10.1016/j.procs.2017.10.079.

S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy (2012). Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain. International Journal of Engineering Research and Applications,2(3),2632-2637.

SistlaVasundhara Devi and Harika Devi Kotha (2019). AES encryption and decryption standards. J. Phys.: Conf. Ser. 1228 012006.

Stuti Goel et al.,(2013). A Review of Comparison Techniques of Image Steganography. Global Journal of Computer Science and Technology, 13(4).

Tayana Morkel et al.,(2005). An Overview of Image Steganography. Proceedings of the ISSA 2005 New Knowledge Today Conference, South Africa.

Vishwakarma Singh, Janarthanan.S, Ujjwal Kumar Roshan, Nandan Vaid (2023). A Secure Web-Based Android Chat Application Using The AES Encryption Algorithm. 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N).

Zaid Al-Omari, Ahmad T. Al-Taani (2015). A Survey on Digital Image Steganography. ICIT 2015 The 7th International Conference on Information Technology, doi:10.15849/icit.2015.0016.