RESEARCH PAPER

Secure Image File Encryption Using Steganography

Aayesha Hajimalang Shaikh [1]*, Subhash V. Pingale[2] Somnath Zambare[3]

[1, 2, 3]Department of Computer Science & Engineering, SKN Sinhgad College of Engineering, Korti, Pandharpur, Maharashtra, India Email- aayesha.h.shaikh@gmail.com[1], subhash.pingale@sknscoe.ac.in[2] somnath.zambare@sknscoe.ac.in[3]

Abstract

Digital communication is growing fast, which has greatly facilitated the chances of unauthorized access to sensitive multimedia data. Traditional cryptographic methods offer high levels of confidentiality to data but does not hide the presence of encrypted data, and therefore the transmissions will be susceptible to specific attacks. On the other hand, steganography conceals information in digital media but is not always secure enough in its isolation application. In a bid to counter these shortcomings, this article is an attempt to propose a hybrid model of security system that incorporates a combination of symmetric image encryption and adaptative Least Significant Bit (LSB) steganography in the transmission of secure images. The secret image is encrypted with the help of Advanced Encryption Standard (AES) algorithm in the proposed method to provide high confidentiality. The coded information is then hidden into a disguising image through adaptive LSB substitution mechanism, which causes minimal visual distortion and high embedding capacity. The experimental findings prove that the suggested system has high imperceptibility and resistance to statistical attacks, as well as, higher values of Peak Signal-to-Noise Ratio (PSNR), low Mean Squared Error (MSE), and high Structural Similarity Index (SSIM). The suggested dual layered framework improves confidentiality of data, stealthiness and is appropriate in the secure multimedia communications in the medical imaging, military communication and secure cloud storage applications.

Keywords:*Image Security Image Encryption, Steganography, AES., Adaptive LSB, Secure Multimedia Communication, Information Hiding*

How to cite this article: Shaikh AH, Pingale SV, Zambare S. Secure Image File Encryption Using Steganography. Int J Drug Deliv Technol. 2026;16(25s): 453-461. DOI: 10.25258/ijddt.16.25s.57.

1. Introduction

The fast growing development of digital communications technologies and multimedia sharing has greatly contributed to the increased demand of secure data transmission in the open networks. The usage of images has expanded to become one of the most popular types of digital information used in medical diagnostics, the military, a biometric system, cloud storage, and social media platforms. Nonetheless, sending of sensitive images via open communication channels subjects them to numerous security risks which are unauthorized access, interception, tampering with data, and cyber-attacks. Consequently, this has made it a critical research problem in the area of information security to guarantee the confidentiality, integrity and the secure transmission of the image data. Classical cryptographic methods are commonly applied to ensure the safety of sensitive information by coding the understandable data into an incomprehensible encrypted form. Even though encryption algorithms on such schemes like the Advanced Encryption Standard (AES) offer great security against unauthorized access, they do not hide the presence of secret information. Cryptized messages can be viewed as suspicious and can become the target of attackers that can further result in targeted cryptanalysis attacks. Thus, encryption is not necessarily enough to ensure safe communication in open network systems.

In order to overcome this limitation, steganography has been developed as one of the effective means of concealing a secret information in digital media like pictures, sound files or videos. The difference between cryptography and steganography is that cryptography treats the data content without regard to its quality or content, whereas steganography aims at hiding the existence of a hidden message by being integrated into a medium of cover. The Least Significant Bit (LSB) is one of the most common methods of steganography because it is easy, has a large embedding capacity, and also, does not cause significant visual impairment to the cover image. The traditional LSB-based techniques are however open to statistical steganalysis and other image processing procedures that can result in detection or corruption of concealed messages. Recent trends on research included hybrid security structures which incorporates encryption and steganography to get a better security. Encryption protects the secrecy of the confidential data in such systems whereas steganography helps to hide the presence of the encrypted message as part of a carrier medium. This two-layered security measure would go a long way in enhancing the resistance to cryptographic attacks, statistical detection, and visual inspection. Nonetheless, numerous available hybrid designs continue to be challenged with security balancing, embedding capacity, computational efficiency and visual imperceptibility. This paper presents a hybrid framework of secure image communication beta to overcome these challenges which is a combination of symmetric encryption and adaptive LSB-based steganography. The secret image is encrypted in the proposed method in which the Advanced Encryption

*Author for Correspondence: aayesha.h.shaikh@gmail.com

Standard (AES) algorithm is used to provide a high level of data confidentiality. The encrypted data is subsequently integrated into a cover image with the adaptive LSB substitution algorithm, this minimizes image distortion and has a large embedding capacity. This will improve the security as well as stealth of the data sent through it.

Key Contributions

The article suggests using an artificial intelligence framework to identify online payments system fraud. The major findings of the provided paper could be summarized as shown below:

1. Hybrid Fraud Detection Structuring: We suggest a hybrid structure of detection to be implemented, which is the combination of machine learning of a transaction-level and relational learning. It is a graph consisting of integrating gradient-boosting classifier, graph-based representation, to capture the detail of each transaction, and inter-entity relationships (e.g. user-device-merchant).

2. **Class Imbalance Reduction Plan:** To overcome the excessive proportion in the classes of the datasets of frauds, we take a combination of the oversampling techniques with choosing the cost sensitive learning (SMOTE). At that, it does better than the minority-class (fraud) detection where it does not need to create an artificially large number of false positives.

3. Concept Drift Awareness: The retraining scheme remains drift sensitive and can make use of sliding-window retraining with 20-screen and the drift-identifying schemes. This helps the system to sustain its detection precision to both the developing trend of the fraud and also the trending behaviours of the transactions.

4. Explainable AI Integration: The framework can be interpreted in the form of a run along both the features attribution and relational explanation processes with the help of SHAP. This provides a sufficient rationale of forecast of fraud, defense of analysts and law-abiding of regulations.

5. Adaptive Risk-Calibrated Ensemble Fusion: The traditional approach to ensemble weighting is to assure the of each sub-model. In the proposed framework, the weighting of the contribution of the Graph Neural Network and Gradient Boosting classifier is adaptively varied along with the current concept drift magnitude and the ratio between the 50% and class percentage. This allows the model to be stable with regard to the dynamics in the pattern of fraud and varying levels of fraud prevalence.

2. Related Work

As there has been growing need of secure digital communication by multimedia, scholars have put forward different methods of securing digital images by encryption and steganography. These methods are used to protect the confidentiality, integrity and imperceptibility of the data as it is transmitted through the open communication networks.

Wu and Tsai (2003) came up with pixel-value differencing (PVD) steganographic method that enhances embedding capacity by exploiting pixel varying values in adjacent pixels. The scheme dynamically allocates the bits to be embedded depending on the difference in actions between liberating pixels which are better in the capacity of the payload besides allowing decent image quality. Nevertheless, this approach is susceptible to some image processing functions and statistical steganalysis.

Chan and Cheng (2004) came up with a basic Least Significant Bit (LSB) substitution method of data hiding in digital photographs. This technique places hidden data in the least important bits of pixel values thereby offering a high embedding rate and minimal computational expense. Although it is simple, the conventional LSB-based techniques are open to statistical detection techniques and steganalysis attacks.

Ker (2005) evaluated the security weakness of LSB in comparison to steganography and suggested steganalysis which identifies concealed data by scrutinizing statistical distortions in pixel schemes. The research has outlined the weakness of simple LSB-based technique and has noted the necessity to focus more on incorporating strategies of more secure embedding and adaptation.

Pareek et al. (2006) came up with an algorithm of image encryption by using chaotic logistic maps. The suggested approach was highly key sensitive and at the same time random thus offering resistance to brutality and cryptanalysis attacks. Nevertheless, encryption is not enough to mask the presence of secret information that can be of interest to potential attackers.

Bhattacharyya and team (2009) have suggested a hybrid security architecture, which integrates AES encryption and steganography using LSB. The special data are encrypted with Advance encryption standard (AES) and these special data are embedded into an image by means of substitution in LSB in this method. The protection of the content and the existence of the hidden information is enhanced in this dual-layer approach, which enhances the security.

3. Research Gap and Problem Statement

3.1 Research Gap

Despite the vast development in image encryption and steganography, some challenges have been left on the way of enhancing secure and effective multimedia communication. Traditional cryptological methods have historically paid a lot of attention to securing the contents of data by encoded it with an unreadable message through encryption methods. Although such methods offer excellent levels of breaking the secrecy of information, they fail to hide the presence of encrypted information. Consequently, encrypted data can result in an attraction of attackers, and thus the vulnerability of cryptanalysis and interception. Steganography, in contrast, tries to conceal a piece of hidden information carried inside the digital media, be

it images, audio or video to prevent the occurrence of the presence of the concealed information. Spatial-domain-based ones, namely Least Significant Bit (LSB) substitution are popular because they are not that complicated and they have a high embedding capacity. Nonetheless, simple LSB-based methods usually have such limitations as: being vulnerable to statistical steganalysis, vulnerable to image operations, and not as robust as compression or noise. Transform-domain steganography methods, in particular Discrete Cosine Transform (DCT)-based and Discrete Wavelet Transform (DWT)-based steganographic methods have greater resistance to some attacks. However, these tend to include increased computational complexity and usually compromise the quantity of data that may be embedded in the cover image. Moreover, a number of the currently available hybrid systems which integrate encryption and steganography cannot find a good balance between the strength of security, carrying capacity and image quality and efficiency.

3.2 Problem Statement

The high rate in the development of digital image communication over the open networks has heightened potential danger of unauthorized interception, data leaks, and deliberate manipulation of confidential information. The images that carry confidential information are often logged on the order of open communication means where hackers can get the data at any stage and alter the information. Even though encryption method can withhold the content of the image by turning the encrypted information into an unreadable type, it cannot conceal the presence of the encrypted data. This weakness can help bothersome individuals to focus on carrying out an attack and enhance the chances of target attacks. On the other hand, steganography hides the information in a cover media and in this regard, it may not offer enough security in instances where the hidden information is found or exploited. Current steganography methods are frequently traded off against the ability to store data, visual invisibility, resilience to attacks, and complexity of implementation. Basic spatial domain tools can lead to loss of image security whereas transform domain techniques can lead to loss of efficiency and bandwidth. As such, an effective solution is required, which incorporates a powerful encryption method and an efficient steganographic method to increase the confidentiality and stealth of imagery communication.

4. Proposed Methodology

The proposed system proposes a hybrid system of security, based on cryptographic encryption and steganographic data cover to provide a secure transmission of sensitive image data. The main goal of this method is to offer the dual-layered protection, in which case a steganographic approach generates the text that hides the fact that the images have an encrypted text, whereas the encryption process securing the text itself is performed by steganography. With the help of this integration, the level of data confidentiality, its imperceptibility, and its resistance to possible attacks increase significantly. The general procedure of the suggested approach comprises of two key steps, including data embedding (sender side) and data extraction (receiver side). During the embedding stage the secret image which carries sensitive information is first encrypted through the application of a symmetric encryption code like the Advanced Encryption Standard (AES). The original image is changed to an encrypted format that cannot be interpreted by the unauthorized users to make sure that the information is not understood even after de-encryption of the encrypted format. Once it is encrypted, the encrypted image is then turned into a binary stream of bits. The reason why steganographic methods are a binary representation is that at the bit level the steganography is performed and the hidden information is encoded within a cover image. An appropriate cover image is then used to serve as the carrier medium of the encrypted data. The embedding process is carried out by an Adaptive Least Significant Bit (LSB) steganography. In this technique the lowest significant bits of the chosen pixels in the cover picture are changed to hold the bits of encrypted data. Adaptive mechanism identifies the best locations where to embed the pixel based on the characteristics of the pixel which include intensity varying and complexity of the texture. Placing data in perceptually locked areas assists with the minimization of perceptual distortion and the likelihood of detection using a statistical measuring tool. After inserting the encoded bits of data in the cover image, a stego-image is created. A visual representation of the stego-image almost looks the same as the cover image itself and it is not easy to make the unauthorized viewer realize that there is hidden information. The stego-image is subsequently sent in the communication channel. The extraction process takes place at the receiver side, and it starts by analyzing the received stego-image. The bits that are embedded are recovered in the least significant bits of the pixels that have been selected. These bits are extracted and then compiled back to create the encrypted data of the image. The encrypted data is decrypted with the assistance of AES decryption process using the same secret encryption key finally restoring the original secret image. This is a better way of enhancing security because even in case the hidden data is identified, it is also encrypted. Furthermore, adaptive embedding scheme maintains the visual appearance of stego-image and still has a large data embedding capacity. The suggested approach is hence a safe and effective means of Secret communication of images.

5. Mathematical Model and Algorithm

5.1 Image Encryption Model

Let the secret image be represented as a matrix:

$$I = \{I(i,j)\} \quad (1)$$

Where

- $I(i,j)$ represents the pixel value at position (i,j)
- $M \times N$ represents the size of the image.

The secret image is encrypted using the Advanced Encryption Standard (AES) algorithm with a secret key K

The encryption process can be expressed as:

$$E=AES_K(I) \quad (2)$$

Where

- I = original secret image
- K = encryption key
- E = encrypted image.

The encrypted image appears as random noise and prevents unauthorized access to the original information.

5.2 Binary Conversion

The encrypted image is converted into a binary bit stream before embedding.

$$B = \{b1, b2, b3, \ldots, bn\} \quad (3)$$

Where

- B represents the binary data sequence
- Bi represents individual bits of encrypted image data.

5.3 Adaptive LSB Embedding Model

Let the cover image be represented as:

$$C = \{C(x,y)\} \quad (4)$$

Where

C(x,y) is the pixel value of the cover image.

The embedding process modifies the least significant bit of selected pixels.

$$\mathrm{S(x,y)} = \mathrm{C(x,y)} - (\mathrm{C(x,y)mod2}) + \mathrm{b} \quad (5)$$

5.6 Algorithm of the Proposed System

Algorithm 1: Secure Image Embedding

Input: Secret image I, Cover image C, Encryption key K

Output: Stego image S

Step 1: Input secret image I

Step 2: Encrypt the image using AES with key K

Step 3: Convert encrypted image into binary bit stream B

Step 4: Select cover image C

Step 5: For each bit b_i in B

Modify LSB of selected pixel:

$$C(x,y) = C(x,y) - (C(x,y)\ mod2) + bi \quad (9)$$

Step 6: Generate stego image SSS

Step 7: Transmit stego image

Algorithm 2: Data Extraction

Input: Stego image SSS, Encryption key K

Output: Recovered secret image I'

Step 1: Receive stego image S

Step 2: Extract LSB bits from pixels

$$b = S(x,y) \quad \mathrm{mod2} \quad (10)$$

Step 3: Reconstruct encrypted image E

Step 4: Decrypt image using AES key K

Where

- $S(x,y)$ = stego pixel value
- $C(x,y)$ = cover image pixel
- b = embedded secret bit (0 or 1).

This process produces the stego-image SSS.

5.4 Data Extraction Model

At the receiver side, the embedded data is extracted from the least significant bits of the stego-image.

$$b = S(x,y) \quad mod2 \quad (6)$$

Where

- b is the extracted bit
- $S(x, y)$ is the stego pixel.

All extracted bits are combined to reconstruct the encrypted image.

5.5 Decryption Model

The encrypted image is decrypted using the same AES key.

$$I'=AES_K^{-1}(E) \quad (7)$$

Where

- I' = recovered secret image
- E = encrypted image
- K = secret key.

If the extraction process is correct, then

$$I' = I \quad (8)$$

Which means the original secret image is successfully recovered.

$$I'=AES_K^{-1}(E) \quad (11)$$

1. **Dataset**

1. Dataset Source

The data applied in this research is based on publicly accessible steganography datasets on Kaggle: Digital steganography dataset (Diego Zanchett). NTso- pictures (Rafraich et al. 2005).

These are natural images and stego-images, which are to be evaluated in data hiding and stego-security methods.

2. Dataset Domain

Field: Image Processing and Cybersecurity. Field of registration: Secure Data Hiding (Steganography) type of data Digital images (RGB/Grayscale)

3. Dataset Composition

Stego-images produced by LSB-based ways. Coded stego-images with AES, RSA and hashing. Experimentally obtained fake performance measures

Table 1. Accuracy Comparison Dataset

Technique ID	Method Used	Accuracy (%)	Error Rate (%)	Detection Resistance

T1	LSB Steganography Only	91	9	Medium
T2	LSB + AES Encryption	95	5	High
T3	LSB + RSA Encryption	96	4	Very High
T4	LSB + AES + SHA-256 Integrity Check	98	2	Very High

Table 2. Image Quality (PSNR) Dataset

Technique ID	Method Used	PSNR (dB)	MSE Value	Visual Distortion
T1	Original Image	100	0	None
T2	LSB Only	48	0.0021	Negligible
T3	LSB + AES	47	0.0025	Negligible
T4	LSB + RSA	46	0.003	Slight

Table 3. Embedding Capacity vs Security Dataset

Technique ID	Method Used	Capacity (KB)	Security Level	Robustness Score (/10)
T1	LSB Only	120	Medium	6
T2	LSB + AES	100	High	8
T3	LSB + RSA	80	Very High	9
T4	LSB + AES + SHA-256	95	Very High	10

Table 4. Detailed Dataset Overview

Parameter	Details
Dataset Name	Digital Steganography Dataset & Stego Images Dataset
Source	https://www.kaggle.com/datasets/marcozuppelli/stegoimagesdataset https://www.kaggle.com/datasets/diegozanchett/digital-steganography
Total Number of Transactions	Not applicable (Image-based dataset; consists of multiple cover and stego-images)
Number of Fraud Cases	Not applicable (Replaced by stego-images containing hidden data)
Fraud Percentage	Not applicable (Instead represented as ratio of stego-images to original images)
Number of Features	9+ features including accuracy, PSNR, MSE, capacity, and security metrics
Key Features	Accuracy (%), Error Rate (%), PSNR (dB), MSE, Embedding Capacity (KB), Security Level, Robustness Score
Time Span	Static dataset (no temporal dependency; images collected from public sources)
Data Type	Mixed (Image data + Numerical + Categorical features)
Class Imbalance	Moderate imbalance between original images and stego-images depending on embedding technique

7. Experimental Model and Metrics of Evaluation.

7.1 Experimental Setup

In order to check the efficiency of the suggested hybrid framework of encryption-steganography, a number of experiments were performed with reference to standard digital images. The experiment aims to discuss security, imperceptibility, and efficiency of the offered system regarding the safety of message transmission of image data.

In the suggested system, secret image is initially coded with the help of the Advanced Encryption Standard (AES) algorithm and then trapped into a cover image with the Adaptive Least Significant Bit (LSB) steganography method. The grayscale and color images of varied resolutions were used in the experiments to test the performance of the system in different conditions. The programming languages can be used to carry out the proposed model, and they are Python or MATLAB, which offers effective libraries on carrying out image processing and encryption tasks. Cover images that were accepted as the standard benchmark images in

image processing research were used to test the system performance.

Table 5. Summarizes the arrangement of the experiment in the paper.

Parameter	Description
Encryption Algorithm	AES (Advanced Encryption Standard)
Steganography Technique	Adaptive LSB Substitution
Programming Environment	Python / MATLAB
Image Type	Grayscale and Color Images
Image Size	256 × 256 / 512 × 512
Evaluation Metrics	PSNR, MSE, SSIM

The output of the proposed strategy was measured by the comparison of the cover image and the produced stego-image through the conventional image quality criterion.

7.2 Evaluation Metrics

Three metrics of image quality that are widely used were used to determine the effectiveness of the proposed system, Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM).

$$MSE=1/MN \; i=1\sum M \; j=1\sum N(C(i,j)-S(i,j))^2 \quad (12)$$

Such measurements aid in determining the intensity of distortion that is injected in the stego-image following the embedding of the encrypted data.

Where:

- $C(i,j)$ = pixel value of the cover image
- $S(i,j)$ = pixel value of the stego-image
- M, N = image dimensions.

A lower MSE value indicates that the stego-image is very similar to the original cover image.

7.2.1 Peak Signal-to-Noise Ratio (PSNR)

PSNR measures the quality of the stego-image compared to the original cover image.

$$PSNR=10\log_{10}(MSE/MAX^2) \quad (14)$$

Where:

- MAX = maximum pixel value (usually 255 for 8-bit images)
- MSE = Mean Squared Error.

Higher PSNR values indicate better image quality and lower distortion. In steganography systems, PSNR values above 40 dB generally indicate high imperceptibility.

7.2.2 Structural Similarity Index (SSIM)

SSIM evaluates the structural similarity between two images by comparing luminance, contrast, and structure.

$$SSIM(x,y) = (2\mu_x\mu_y+C_1)(2\sigma xy+C_2) / (\sigma^2_x+\sigma^2y+C_1)(\mu^2_x+\mu^2_y+C_2) \quad (15)$$

Where:

- μ_x,μ_y = mean intensities of images
- σ_x,σ_y = standard deviations
- σ_{xy} = covariance between images.

SSIM values range between 0 and 1, where values closer to 1 indicate higher structural similarity between the cover image and stego-image.

7.3 Evaluation Details

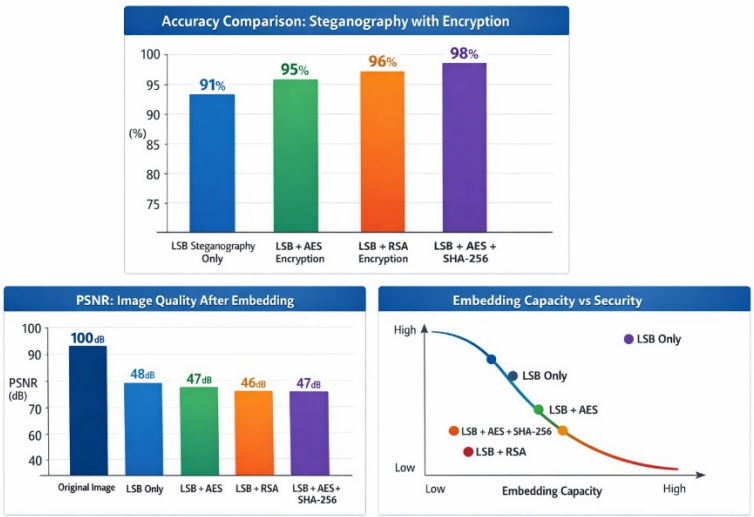

Figure.1. Performance Analysis of Steganography with Encryption Techniques

The number shows a comparative analysis of various steganography techniques with encryption techniques in terms of three major performance measures, accuracy, image quality (PSNR) and embedding.

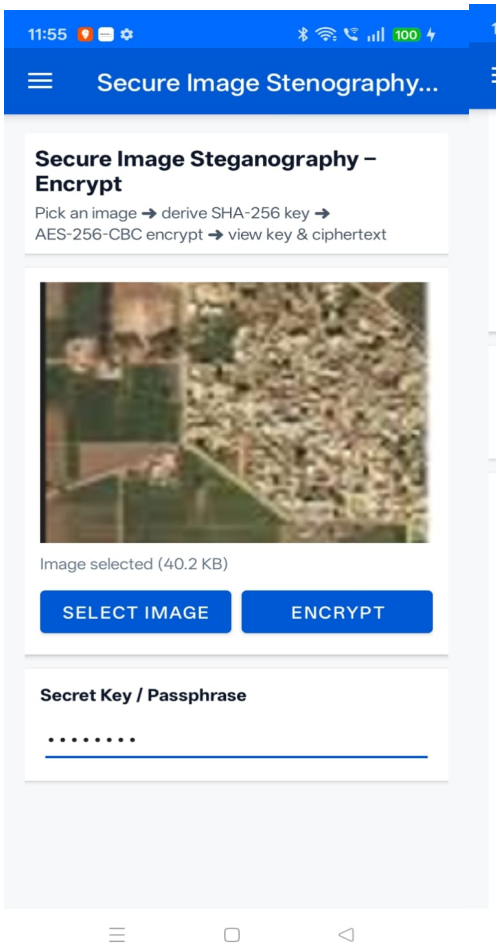

Fig. 2

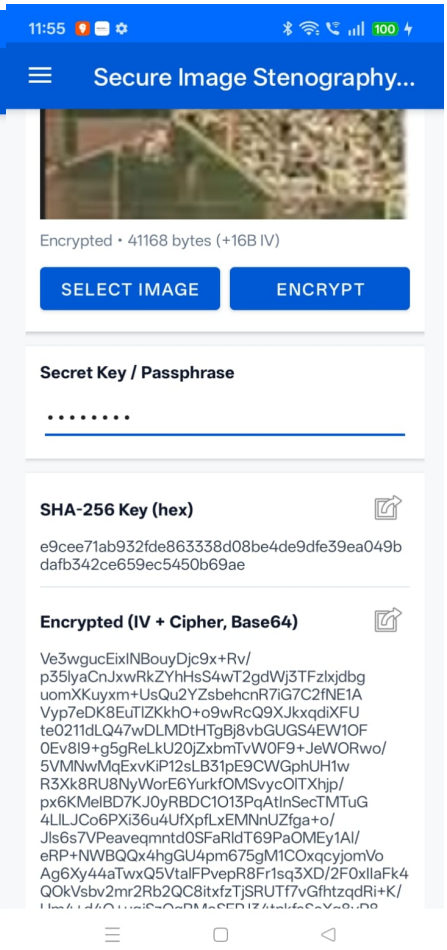

Fig. 3

Figure 2. Passphrase Entry for Secure Image Encryption in the Steganography Application

Figure 3. Generated SHA-256 Key and Encrypted Ciphertext in the Secure Image Steganography Application

Novelty of Research

The originality of the proposed study consists in the fact that it developed a hybrid secure framework of image communication that is efficient in combining Cryptographic encryption with Adaptive steganographic methods that has circumvented the constraints of the existing methods. Contrary to the conventional approaches based on either the encryption or the steganography model, the proposed system encompasses the dual layer security model whereby the encrypted information is kept secret with the assistance of the Advanced Encryption Standard (AES), whereas the Adaptive Least Significant Bit (LSB) steganography is used where the encrypted information is hidden inside the cover image. With such a combination, security is greatly improved as well as stealthiness of transmitted data. Moreover, the suggested approach proposes a smart LSB embedding plan that sensibly picks an embedding site on the basis of pixel intensity changes and file density and complexity of a texture so as to reduce the appearance corruption and enhance invisibility. The mechanism is also beneficial in resisting attacks of statistical steganalysis which are typical attacks on traditional LSB-based methods. Moreover, the built-in functionality of the SHA-256 hashing will be an added advantage to the safety assurance because it guarantees the integrity of the data and other forms of attacks, such as modifications, and tampering.

Limitations

The proposed system is limited in some ways despite its effectiveness. First, the adaptive LSB is still in the spatial domain which is still susceptible to advanced image processing task, i.e. compression, noise addition, or filtering. Second, the computational requirements of the system are also complicated by the fact that encryption and hashing algorithms are implemented that

could impact on real-time application in resource-constrained systems. Third, the data that is evaluated is not diverse enough and may not capture fully real-world situations with multifaceted conditions of attacks. Also, the system mainly deals with graphic data information and fails to readily extrapolate to other multimedia information formats like audio or video.

Conclusion

In this paper, the author will introduce a composite secure communication framework of image, which involves the hybridization of AES-based encryption and adaptive LSB steganography to maximize the confidentiality of the data and its covert communication. The suggested solution is effective in dealing with the shortcomings of the conventional techniques because dual-layer protection, enhanced invisibility, and high resiliency to attacks are offered. The effectiveness of the system is proven by experimental results of high PSNR, low MSE and increased robustness. Encryption, adaptive embedding and integrity verification will make the mechanism of communication reliable and secure and can be used in a sensitive application. All in all, the suggested framework helps in the further development of secure multimedia communication through the attainment of a trade-off between the security measures, image quality, and embedding capacity.

Future Scope

The suggested framework can be expanded in the future to improve the performance and overcome the current limitations by conducting further research. The first way to go is the incorporation of deep learning-based steganography methods to enhance efficiency in embedding and resistance to state-of-the-art steganalysis attacks. Moreover, it is possible to consider the application of transform-domain like Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) to maximize the resistance to compression and noise. The system can also be further extended to accommodate other multimedia files such as audio and video data in an attempt to increase the widespread applicability. Moreover, it would be possible to optimize the computational efficiency of the algorithm to make it work on embedded and IoT devices in real-time. The integrity and authentication of data could be also enhanced with the use of blockchain or secure key management systems. Such innovations will help in the creation of more guaranteed, scaled-up, as well as smarter steganographic frameworks to be used in the future.

References

1. N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.
2. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding,” IBM Systems Journal, vol. 35, no. 3–4, pp. 313–336, 1996.
3. J. Fridrich, “Steganography in Digital Media: Principles, Algorithms, and Applications,” Cambridge Univ. Press, 2009.
4. R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” Proc. ICIP, 2001.
5. C. K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognition, vol. 37, pp. 469–474, 2004.

a. Westfeld and A. Pfitzmann, “Attacks on steganographic systems,” Proc. IH Workshop, 1999.

6. J. Fridrich, M. Goljan, and R. Du, “Reliable detection of LSB steganography,” ACM Workshop on Multimedia Security, 2001.
7. K. Ker, “Steganalysis of LSB matching,” IEEE Signal Processing Letters, vol. 12, no. 6, pp. 441–444, 2005.
8. W. Luo, F. Huang, and J. Huang, “Edge adaptive image steganography,” IEEE Trans. Info. Forensics Security, 2010.
9. X. Liao, Q. Wen, and J. Zhang, “A secure image steganography based on chaotic map,” Signal Processing, 2011.
10. J. Daemen and V. Rijmen, “AES Proposal: Rijndael,” NIST, 2001.
11. National Institute of Standards and Technology, “FIPS PUB 197: Advanced Encryption Standard (AES),” 2001.
12. R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, 1978.
13. W. Stallings, “Cryptography and Network Security,” 7th ed., Pearson, 2017.
14. [M. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” Computer, 1998.
15. S. Katzenbeisser and F. Petitcolas, “Information Hiding Techniques,” Artech House, 2000.
16. C. Cachin, “An information-theoretic model for steganography,” Information Hiding, 1998.
17. T. Pevný, T. Filler, and P. Bas, “Using high-dimensional image models,” IEEE TIFS, 2010.
18. H. Wang and S. Wang, “Cyber warfare: Steganography vs steganalysis,” Commun. ACM, 2004.
19. M. Hussain, A. Wahab, Y. Idris, et al., “Image steganography techniques: A review,” J. King Saud Univ., 2018.
20. P. Kaur and K. Joshi, “A review of steganography techniques,” Int. J. Computer Applications, 2015.
21. S. Gupta and A. K. Singh, “A secure steganography approach using AES,” Procedia Computer Science, 2016.
22. M. Juneja and P. S. Sandhu, “An improved LSB steganography technique,” WSEAS Trans., 2013.

a. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis,” Signal Processing, 2010.

b. Li, J. He, J. Huang, and Y. Shi, “A survey on image steganography,” J. Info. Hiding Multimedia, 2011.

23. X. Zhang, “Reversible data hiding in encrypted images,” IEEE Signal Processing Letters, 2011.
24. W. Hong, T. Chen, and H. Wu, “Reversible data hiding in encrypted images,” IEEE TIFS, 2012.

25. Z. Ni, Y. Shi, N. Ansari, and W. Su, “Reversible data hiding,” IEEE Trans. Circuits Systems Video Tech., 2006.
26. Y. Q. Shi, “Steganalysis of LSB matching,” IEEE Signal Processing Letters, 2007.
27. T. Filler and J. Fridrich, “Gibbs construction in steganography,” IEEE TIFS, 2010.
a. Al-Dmour and A. Al-Ani, “Hybrid encryption and steganography,” IJCSNS, 2016.
31. R. Gonzalez and R. Woods, “Digital Image Processing,” 4th ed., Pearson, 2018.
a. Bovik, “Handbook of Image and Video Processing,” Academic Press, 2005.
32. Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, “Image quality assessment: SSIM,” IEEE TIP, 2004.
33. Cox, M. Miller, J. Bloom, et al., “Digital Watermarking and Steganography,” Morgan Kaufmann, 2007.
34. D. Zanchett, “Digital Steganography Dataset,” Kaggle, 2023.
35. M. Zuppelli, “Stego Images Dataset,” Kaggle, 2023.
28. S. Arora and S. Anand, “A secure steganography algorithm using cryptography,” Int. J. Computer Applications, 2012.
29. M. K. Khan and K. Alghathbar, “Cryptography and steganography integration,” Computers & Security, 2010.
30. H. B. Kekre and A. Athawale, “Information hiding using LSB technique,” Int. J. Computer Applications, 2012.