Journal of Science, Computing and Engineering Research (JSCER)
Volume-7, Issue-11, November 2024.
DOI: *https://doi.org/10.46379/jscer.2023.071102*
ISSN: 2708-1079

Dual-Layered Security Using cryptography and Image Steganography

[1] M.SASIKALA,[2]SHYAM SUNDHAR,[3] M.VISWA,[4] P SEVUGAMOORTHY ,[5] V.RAJAPRABHAKARAN

[1]ASSITANT PROFESSOR,[2-5] UG STUDENTS, K.L.N. COLLEGE OF ENGINEERING, POTTAPALYAM, SIVAGANGAI, 630612

Article Information

Received : 05 Nov 2024
Revised : 08 Nov 2024
Accepted : 12 Nov 2024
Published : 16 Nov 2024

Corresponding Author:

N Shyam Sundhar
Email: shyamsundharnaga @gmail.com

Abstract— This paper proposes a dual encryption technique for maximizing message secrecy in practice using combination of cryptography with steganography. First, we encrypt our secrets using Advanced Encryption Standard (AES), which is a strong public key cryptosystem, and then we hide the data in image files using image steganography. In this way, embedded messages encrypted by AES were placed in the least significant bits (LSB) of pixel which are difficult to detect using Conditional LSB Substitution technique. This two-layer protection makes it impossible to decrypt whatever is not authorized, and the chances of casual discovery are greatly reduced. Through a set of performance tests, the effectiveness of the strategy is validated with the resulting parameters: security and covert communication. It has been proved that combination of AES and LSB steganography provides a quite efficient and comprehensive means of secure communication and can be employed in scenarios that require a high level of confidentiality.

Keywords: AES, Image Steganography, Conditional LSB Substituion

Citation: M.SASIKALA,N.SHYAMSUNDHAR,M.VISWA,P.SEVUGAMOORTHY,V.RAJAPRABHAKARAN "Dual-Layered Security Using cryptography and Image Steganography itle of the paper", Journal of Science, Computing and Engineering Research, 7(11), November 2024.

I.INTRODUCTION

Within the modern era of constant communication, which has shifted into the online world, the use of message secrecy has been absolutely important. Considering that secret info can be found in the channels employed, compliance with confidentiality and data integrity is of utmost importance in avoiding exposure to unauthorized persons. However, even though secret messages are usually concealed with effective yet detectable methods such as encryption, such methods as hiding data in images do exist. Therefore, this project suggests a new method of protecting sensitive data by integrating encryption with image content embedding methods, thereby creating a more secure environment. The process of transmitting secure data is achieved through AES encryption that is a symmetric key algorithm encrypting plain text into cipher text that is indecipherable without a key. However, in the modern world, data breaches can occur at any point due to hacking. In such situations where the information is at risk, we can utilize the image steganography where images are used to transmit information while concealing the actual essence of the message. In this project, we make use of the least significant bit (LSB) as a method for embedding information within images and the Conditional LSB Substitution technique as the method for embedding AES ciphered messages in image pixels' data. Quite this way

II.RELATED WORK

[1] Steganography is the art of conveying a secret message through the cover media in such a way that an eavesdropper does not feel suspicion. The main objective of this work is to present the three levels of security, first being the one of complimenting the secret message, Forward, concealed a complemented secret message in a cover image pixels which are obtained by a random pseudo code generator, and third make use of inverted bit LSB method as a steganographic technique instead of simple LSB, so as to lessen the likelihood of detecting the concealed message. MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are both specialized measures of distance which have been resorted to in assessing the level of dissimilarity between the cover image and the stego image. Results showed that the proposed method gives better performance result than LSB and inverted LSB with higher PSNR and lower MSE.

[2] Image steganography works by embedding a secret image within the cover image in such a way that this embedding remains imperceptible. Most of the existing deep learning-based steganography approaches contain a basis for improving payload capacity, visual appearance, and steganography security features. This, however, doesn't make it easy to lossless retrieve the secret images from stego images that have a relatively high payload capacity. More recently, a few studies have begun to illustrate how invertible neural networks can be used for implementing high capacity image steganography. Unfortunately these techniques have been unable to lossless reconstruct the secret image because information has been irrevocably lost on the output side of the concealing network. In this paper, we describe our efforts in using an INN-based framework for image steganography which is lossless in nature. More specifically, we frame image steganography as an image super-resolution problem which seeks to transform low resolution images into high resolution stego images while embedding a secret image in the process. The feature dimension of the generated stego image matches the total dimension of the input secret and cover images, thereby eliminating the lost information. Furthermore, we designed a bijective secret projection module to encode different secret images into a latent variable which has a simple distribution, enhancing the invisibility of the secret image. Extensive experiments confirm that the secure steganography architecture

[3] This is the art of hiding the message in the cover image so that third parties cannot detect the secret message. This paper introduces a new technology in spatial domain image steganography. The new method hides and recovers long-term data in digital images without changing the size or quality of the original image. The gradient of the image is used to generate image saliency, which represents the amount of energy stored in each pixel in the image. Pixels with higher power are more important are useful for hiding information because their blinding is not sufficient. The cumulative maximum energy matrix is extracted from the saliency image .Then the secret message is stitched to form a steganographic image containing the message. We ensure that the secret information is not visible in the steganographic images and there is very little degradation in image quality. The same algorithm is used to reconstruct the secret messages from the steganographic images. To test the proposed system, experiments are conducted using two types of images and two types of secret data. Experimental results show that the proposed algorithm has high capacity and good concealment, the maximum signal-to-noise ratio (PSNR) is up to 70 and similar models (SSIM) is up to 1.

III.PROPOSED SYSTEM

The proposed system enhances steganographic techniques by using advanced encryption and optimized LSB technique.

The process begins with generating a random salt, a unique value that helps to secure the password used for encryption. This salt is combined with the password through a key derivation function, which applies a hashing algorithm and repeated iterations to create a strong, 256-bit encryption key. Next, a random initialization vector (IV) is created, ensuring that even if the same message and key are reused, the encrypted output will vary. The message is then encrypted with this key, producing a cipher text that is base64-encoded, a format safe for embedding. In the next step, the encrypted message is embedded within an image using steganography. The message is first converted into binary, and a delimiter is added to mark its end. Before embedding, a check ensures the image has enough capacity to store the binary data. Each pixel's color channels are analyzed, and only channels with specific bit patterns are used to store parts of the message. For each eligible channel, a binary bit of the message replaces the least significant bit, which is barely noticeable visually. The final output is an image file that visually appears unchanged but secretly holds the encrypted message within its pixels, adding an additional layer of concealment.

The decryption process begins by loading the encoded image and extracting the hidden binary data bit by bit. Each pixel's color channels are examined to locate channels where the two most significant bits match a predefined pattern, allowing only those channels to be read. The least significant bits from these selected channels are combined to reconstruct the binary message. This binary data is then grouped into bytes and converted to characters until a special delimiter is detected, marking the end of the message. Once extracted, the message is base64-decoded to separate the encrypted components: the salt, initialization vector (IV), and cipher text. Next, the salt is combined with the password in a key derivation function to regenerate the encryption key. Using this derived key and the extracted IV, the cipher text is decrypted with AES in Cipher Feedback (CFB) mode, reversing the encryption process. This reveals the original plaintext message. This multi-step process ensures that only someone with the correct password and knowledge of the extraction criteria can recover the concealed message, safeguarding both its content and location within the image.

IV.SYSTEM DESIGN

1.System Architecture:

Software architecture diagram is a graphical representation of the high-level structure and interactions within a software system. It provides a visual overview of the system's components, their relationships, and how they collaborate to achieve the system's functionality. These diagrams help illustrate how various software components interact and are interconnected.

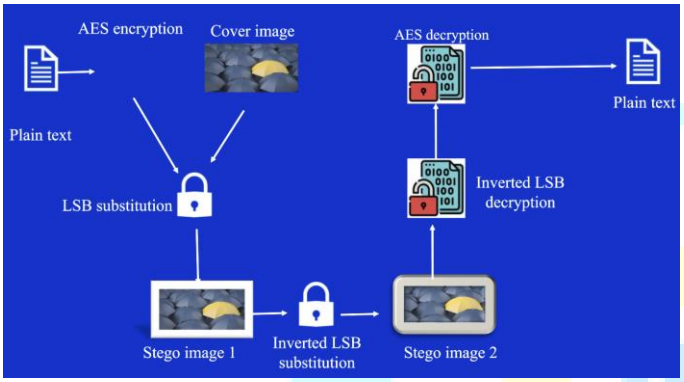

Figure 4.1: Architecture diagram

This architecture diagram outlines a secure communication method that combines cryptographic encryption with image steganography to ensure confidentiality and covert transmission of sensitive information. The process starts with a plain text message that is encrypted using the Advanced Encryption Standard (AES), a reliable symmetric encryption method that secures data by transforming it into an unreadable format. The encrypted message is then concealed within an image through steganography, specifically by embedding the data into the least significant bits (LSB) of the image's pixel data, making the message undetectable to anyone viewing the image. At the receiving end, the recipient employs an conditional LSB extraction technique to retrieve the hidden message, which is then decrypted using the appropriate key to restore the original text. This dual-layered security approach enhances both confidentiality and secrecy, ensuring that even if an unauthorized party intercepts the image, they would need to detect the hidden message and possess the decryption key to access its content, providing a robust solution for secure and covert communication.

2. Dataflow Diagram:

A Data Flow Diagram (DFD) is a visual representation used in software engineering and systems analysis to illustrate the flow of data within a system or process. It provides a structured way to depict how data moves from input sources through processes to output destinations

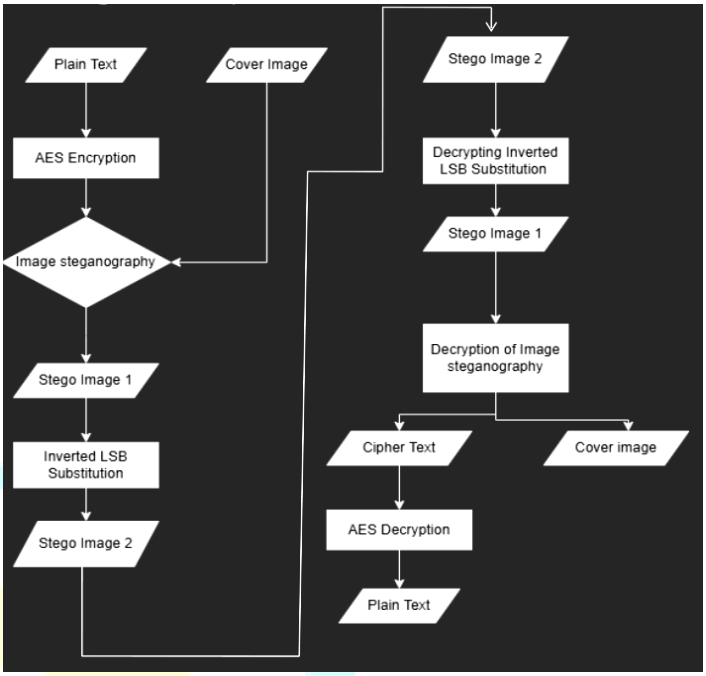

Figure 4.2: Dataflow diagram

The process of secure communication starts with plain text input, which is the message or sensitive information that needs protection. First, this plain text is encrypted using the Advanced Encryption Standard (AES), transforming it into cipher text and securing it from unauthorized access. Next, the encrypted message is cleverly hidden within a cover image through image steganography. This involves embedding the cipher text into the least significant bits (LSB) of the image's pixels, making it nearly invisible.

The outcome of this process is the first stego image, which contains the hidden encrypted message. This stego image is then transmitted to the recipient. Upon receipt, the recipient uses an conditional LSB substitution method to extract the hidden message from the image. After extracting the encrypted message, it is decrypted using the appropriate algorithm, resulting in a second stego image that reveals the encrypted content. Finally, the extracted cipher text is decrypted with the AES algorithm, converting it back to the original plain text. This whole process ensures the confidentiality and secrecy of the message through the combined use of encryption and steganography. In addition to this secure communication method, Data Flow Diagrams (DFDs) serve as powerful tools for systems analysis and design. They provide a structured framework for understanding and optimizing how data flows within a system. Just like a navigator relies on a map, stakeholders use DFDs to gain insights, communicate system requirements, and develop solutions that enhance efficiency and functionality. Overall, DFDs help model data flow, enabling a clearer understanding of system behavior and contributing to the creation of effective systems.

V.RESULT

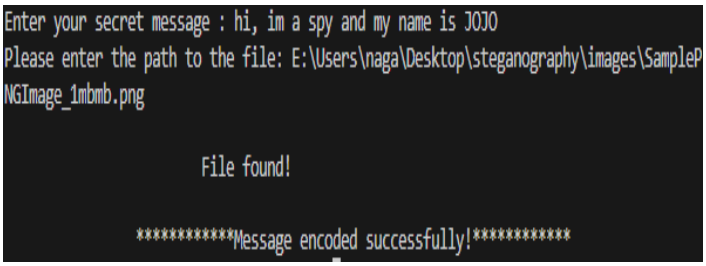

Figure 5.1: Encryption program

In figure 5.1,output reflects a successful dual-layer encryption process that combines AES encryption with image steganography. The process begins with the user entering the secret message, "hi, im a spy and my name is JOJO," which is encrypted using AES, a highly secure encryption standard. The resulting encrypted message is represented as a base64 string. Next, the user specifies the path of an image file, in this case, a PNG image located at `E:\Users\ naga\ Desktop\ steganography\ images\ SamplePNGImage_1mbmb .png`. PNG' file are ideal for steganography due to their lossless compression, which preserves the hidden data without noticeable alterations to the image. The encrypted message is successfully embedded within the image using steganography, a technique that conceals information in images while keeping the visual integrity intact. The program confirms the successful encoding of the message into the image, thus completing a dual security measure where the message is first encrypted and then hidden within an image, ensuring that both its content and existence remain confidential.

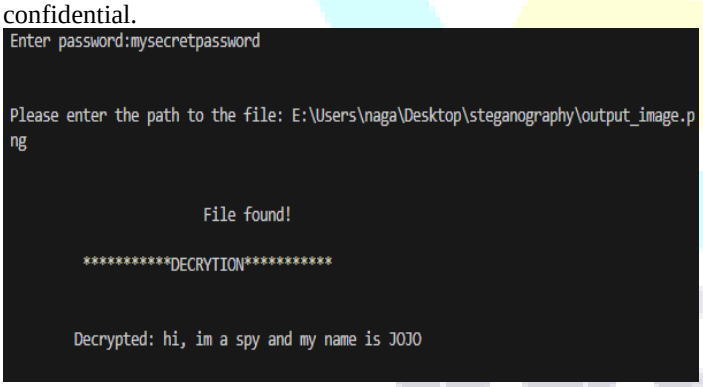

Figure 5.2: Decryption program

In figure 5.2, output demonstrates the successful decryption process from the previously encrypted message using AES and steganography. The user initiates decryption by entering the password "mysecretpassword" and specifying the path to the image file
`E:\Users\naga\Desktop\steganography\output_image.png`, which contains the hidden message. The program confirms that the image file has been found.
The program first extracts the Least Significant Bit (LSB) data from the image.

The extracted string is

```TIJ765dcw47bolZaJ5+TkYkauTntQZ5E1Rh062QnqkzSFo ZzBERNrRGvNngo5+aPmTNC2nIYnDG1LGBr/aEGYg==```

this hidden encrypted message that was previously embedded in the image during the encryption process. After extracting the encrypted message, the program proceeds to decrypt it using AES, with the password provided earlier. The encrypted message is successfully decrypted back to the original text.
The decrypted message is then revealed as

```hi, im a spy and my name is JOJO ```

IMAGE SIZE	PSNR
1mb	84.0764560291561 dB
3mb	90.51832151199753 dB
5mb	91.04099057377198 dB
100kb	74.1115139664977 dB
200kb	77.61284915309918 dB
500kb	83.26413788242019 dB

Figure 5.3: PSNR results

From figure 5.3, PSNR value of 84 dB indicates an extremely high degree of similarity between two images, suggesting that the difference between them is nearly imperceptible. In practical terms, such a high PSNR signifies that the processed image, likely modified for purposes such as steganography, has undergone changes that are visually undetectable. Typically, PSNR values above 40-50 dB are considered excellent, meaning the human eye can barely notice any differences between the original and altered images. With a value as high as 84 dB, the images are virtually indistinguishable, indicating that the process—whether embedding hidden data or some other modification—was done with such precision that the image quality remained almost perfectly intact. In essence, this reflects an ideal scenario where no perceptible noise or degradation has been introduced, preserving the original image's fidelity at an exceptional level.

REFERENCES

[1] S. RAHMAN, J. UDDIN, H. U. KHAN, H. HUSSAIN, A. A. KHAN ANDM.ZAKARYA, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method", 2022,IEEE Access vol. 10, pp. 124053-124075

[2] RUPALI BHARDWAJ, VAISHALI SHARMA, "Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution ",Science Direct , Procedia Computer Science, 2016,Volume 93, Pages 832-838,ISSN 1877-0509

[3] OSAMA FOUAD ABDEL WAHAB ,ASHRAF A. M. KHALAF,AZIZA I. HUSSEIN, HESHAM F. A. HAMED "Hiding Data Using Efficient Combination of RSA Cryptography and Compression Steganography",2021, IEEE Access ,PP10.1109/ACCESS.2021.3060317

[4] RON SHMUELI, DIVYA MISHRA, TAL SHMUELI & OFER HADAR," A novel technique for image steganography based on maximum energy seam", Multimedia Tools and Applications (2024) 83:70907–70920.

[5] Selvan, M. A. (2024). Deep Learning Techniques for Comprehensive Emotion Recognition and Behavioral Regulation.

[6] Selvan, M. A. (2024). SVM-Enhanced Intrusion Detection System for Effective Cyber Attack Identification and Mitigation.

[7] Selvan, M. A. (2024). IoT-Integrated Smart Home Technologies with Augmented Reality for Improved User Experience.

[8] Selvan, M. A. (2024). Multipath Routing Optimization for Enhanced Load Balancing in Data-Heavy Networks.

[9] Selvan, M. A. (2024). Transforming Consumer Behavior Analysis with Cutting-Edge Machine Learning.