International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 06 | June – 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Enhancing Data Confidentiality Through Dual-Layer Cyber Security Tool

K. Satyanarayana Murthy [1], D. Ganesh[2], B. Dhanunjaya Rao[3], B. Yeswanth[4], B. Mohan Sai[5]

[1] Assistant Professor
[2-5] B. Tech Student, LIET
[1,2,3,4,5] Computer Science & Engineering, Lendi Institute of Engineering and Technology, Vizianagaram

---

Abstract - This project introduces a cybersecurity tool that makes use of the complementary fields of cryptography and image steganography. The primary aim is to fortify data confidentiality by implementing robust data hiding algorithms. The tool functions as a dual-layer security mechanism, employing Advanced Encryption Standard (AES) for cryptography and Least Significant Bit (LSB) algorithm for steganography. Through the fusion of these methodologies, the project works to enhance the protection of sensitive information by concealing it within digital images. The utilization of AES ensures a formidable encryption process, while the LSB algorithm facilitates the covert embedding of encrypted data into images. The project offers a promising way to improve data confidentiality with its creative combination of steganographic hiding and robust cryptography, offering an extra layer of defense against potential breaches or cyber threats.

Key Words: Steganography, AES Algorithm, Data Encryption, LSB, Confidentiality, Security

1. INTRODUCTION

1.1. LSB Image Steganography

The word "Steganography" is a Greek term that means "covered or hidden writing". In other terms, Steganography is a technique for concealing information behind a cover medium. Steganography can be performed using text, images, video, audio, or protocol. In our work, we will use digital picture steganography since digital photographs contain a great quantity of redundant data, making it easy to hide messages within image files. Image Steganography requires the following things to complete the work:

- **Cover medium:** It is an image that holds secret message.
- **The Secret message:** it is message or data to be transmitted. It can be plain or encrypted text, images or any other data.
- **The Stego-key:** it is key used to hide the message (may or may not be used).

The data is disguised in such a way that no one notices its presence in the cover medium. The primary purpose of steganography is to conceal the existence of communication.

1.2. Advance Encryption Standard (AES-128 bits)

Advanced Encryption Standard (AES), also known as Rijindael, is used to secure data. AES is a symmetric block encryption that has undergone significant analysis and is commonly used today. AES, a symmetric key encryption method, is utilized with a key length of 128 bits for this purpose. The AES algorithm's qualities include excellent security, mathematical soundness, resistance to all known attacks, high encryption speed, worldwide royalty-free use, and compatibility with a wide range of hardware and software. While DES and 3DES encryption algorithms contain flaws, the AES algorithm has not yet been found to have any. Figure 1 shows the basic construction of AES.

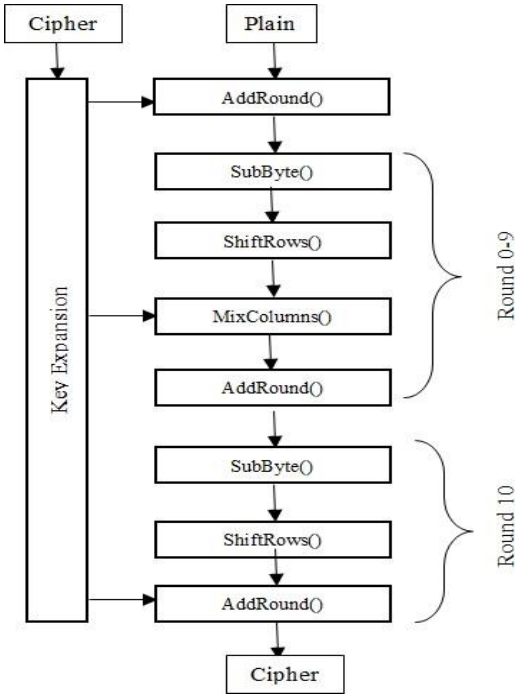

Fig -1: Advanced Encryption Standard Algorithm

2. EXISTING SYSTEM

The current landscape of digital data protection primarily revolves around encryption techniques and protocols to secure data during transmission or while at rest. Encryption, such as AES, scrambles data into an unreadable format for anyone who does not possess the decryption key, providing a strong layer of security. However, encryption alone does not address all aspects of data security, especially concerning the visibility of encrypted data, which can be a beacon for attackers, signifying that there's something worth intercepting or attacking.

3. PROPOSED SYSTEM

Data security is a biggest concern of any organization. In response to the limitations identified in the existing systems, our project introduces a novel approach to data security by seamlessly integrating Advanced Encryption Standard (AES) cryptography with Least Significant Bit (LSB) Image

Steganography. This proposed system is designed to not only secure data through robust encryption but also to obscure the data's very presence, thereby offering a comprehensive solution to the challenges of data confidentiality in the digital age. The cornerstone of the proposed system lies in its dual-layered security protocol. Initially, sensitive information is encrypted using the AES algorithm, renowned for its cryptographic strength and resilience against brute-force attacks. This encrypted data, while secure, remains vulnerable to detection and targeted attacks, which is where the second layer of security LSB Image Steganography comes into play. By embedding the encrypted data into digital images through 8 subtle modifications of the least significant bits of the image pixels, the system effectively renders the encrypted data invisible to all but the most sophisticated analyses. This approach not only capitalizes on the strengths of AES encryption but also mitigates its vulnerabilities by concealing the encrypted data within benign-looking images. Such images can be transmitted or stored without drawing attention, significantly reducing the likelihood of interception or unauthorized access. Moreover, the proposed system is designed with practicality in mind, ensuring that the process of embedding and extracting data does not degrade the image quality perceptibly, maintaining the usability of the steganography technique for real-world applications.

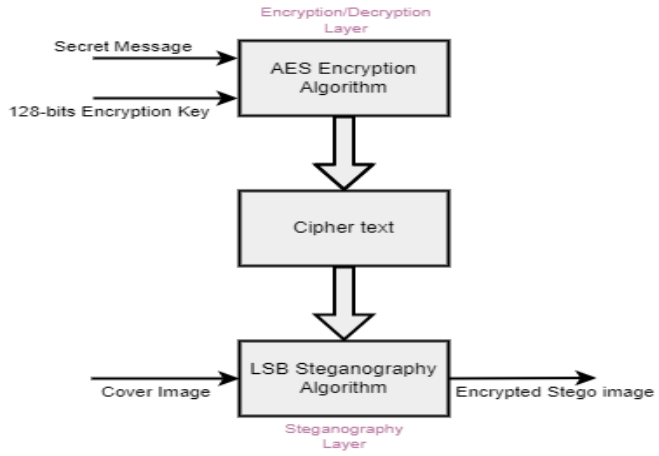

Fig -2: Encryption Process

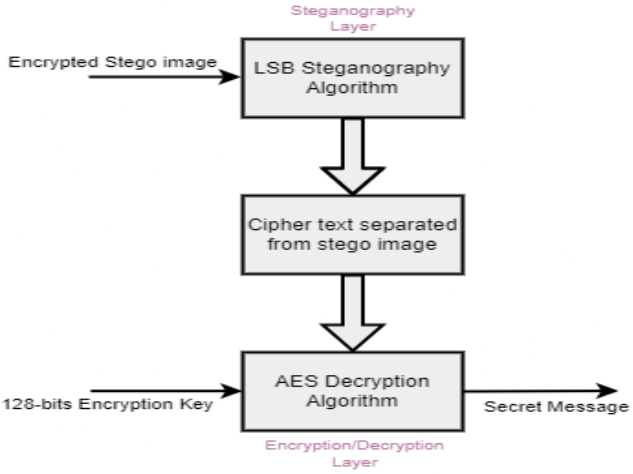

Fig -3: Decryption Process

Encryption/Decryption Layer: The core of first layer in our system is AES 128 bits Encryption algorithm. The output of this layer is a cipher text. We encrypt the secret message with AES algorithm by providing 128 bits phrase key for encryption which is optional but providing a key will give us a secure encrypted text.

LSB Steganography Layer: In this layer, we use the Least Significant Bit picture steganography algorithm. If the LSB of the pixel value of the cover picture C(i,j) is equal to the message bit SM of the secret massage to be inserted, C(i,j) is left untouched; otherwise, set the LSB of C(i,j) to SM. The message embedding procedure is described below:

$$S(i,j) = C(i,j) - 1, \text{ if } LSB(C(i,j)) = 1 \text{ and } SM = 0$$
$$S(i,j) = C(i,j) + 1, \text{ if } LSB(C(i,j)) = 0 \text{ and } SM = 1$$
$$S(I,j) = C(i,j), \text{ if } LSB(C(i,j)) = SM$$

Pixels before Embedding:

Pixel 1: 10001100	01001111	00001111
Pixel 2: 01010100	11010101	11011010
Pixel 3: 11101000	11110110	10000001

Pixels after Embedding "1010011", *i.e.*, alphabet "S" using LSB Algorithm:

Pixel 1: 1000110**1**	0100111**0**	00001111
Pixel 2: 01010100	1101010**0**	1101101**1**
Pixel 3: 1110100**1**	11110110	10000001

In the example before it, just five of the nine bits have changed. It relies on the secret message that will be encoded. There are two sorts of digital images; 8-bit and 24-bit. In an 8-bit picture, only one bit of data can be embedded. However, in a 24-bit image, we can embed three bits of information in each pixel, as demonstrated in the example above. A photograph with 800×600 resolution may store 1,440,00 bits of encoded data. Changing the LSB of each pixel has no effect on the appearance of the original image, therefore the Stego-image seems nearly identical to the cover image. LSB is a basic algorithm with a large payload capacity. In the receiver end reverse process is applied by decrypting the stego image and then decrypting the cipher text.

4. IMPLEMENTATION AND DISCUSSION

The user interface (UI) allows users to input secret message and phrase key for encryption, select cover images for embedding, and initiate decryption processes.

4.1. Encryption Process:

The encryption process involves several phases:

- Data Input: Users input the data they want to encrypt into the system.
- Encryption: The system utilizes the AES encryption algorithm to encrypt the input data, generating ciphertext.
- Steganography: The encrypted data is embedded into digital images using LSB Image Steganography, producing steganographed images

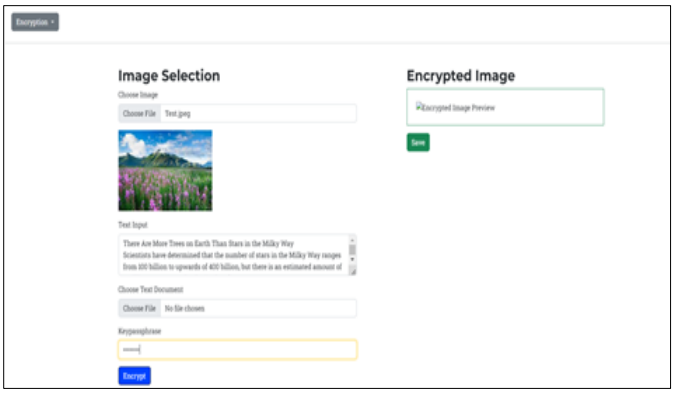

Fig -4: Encryption page layout

4.2. Encryption Results:

After completing the encryption process, the following results are obtained:

- Ciphertext: The encrypted data in ciphertext form.
- Steganographed Images: Digital images containing the encrypted data embedded within them.

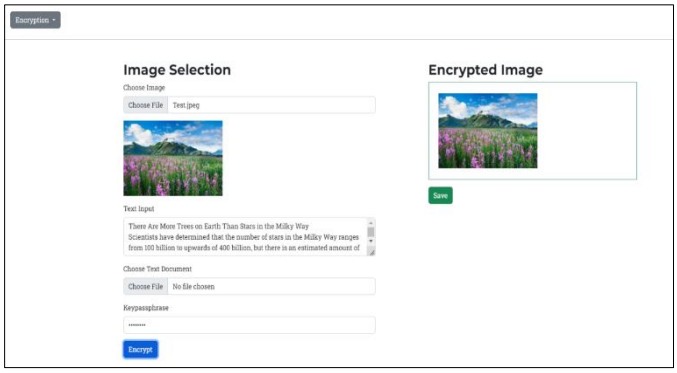

Fig -5: Encryption page Output

The Cipher text will be generated in the backend which is not shared with anyone for the security purposes.
The Cipher text will be in the form of:

f6182db3e285847053b2677e1ca0c06270daa7b3f093c300368
1464451ff8ab38a223c1aabc1e948bcc608a1ba882c130e1a111
6d643741488595d6889b79ed5b1d1560be40f9d2fea1c74bac9
b09b9125794f0a60992009f64a90f80187ea254701692205d4b
1222a1e58ac57780d4a1b10095f6bf2e816f88e3201ab5fff60e4
519e45ae6e0571d0a79ca1e7f8c1963280c643ae1854566863b
873ef276304a3457d22dfee13342b0395e04c8a8ec15f8208538
bc7dad01839409d14d7ec402008cccbf37d849e4d1006fef0dbf
b75a8f93ccfd91b0c5b07ba0e86067bcda8ba655d37dd7c2296
49b72aeaafd0fa7f8bb107c4e054d819b0
3e589bd1215b236bb6024ad21c3bb9bd30a66411e7582a

This won't be the same for all the time.

4.3 Decryption Process:

The decryption process reverses the encryption phases:

- Steganography Extraction: The system extracts the encrypted data from steganographed images using LSB Image Steganography.
- Decryption: The extracted encrypted data is decrypted using the AES decryption algorithm, resulting in plaintext.

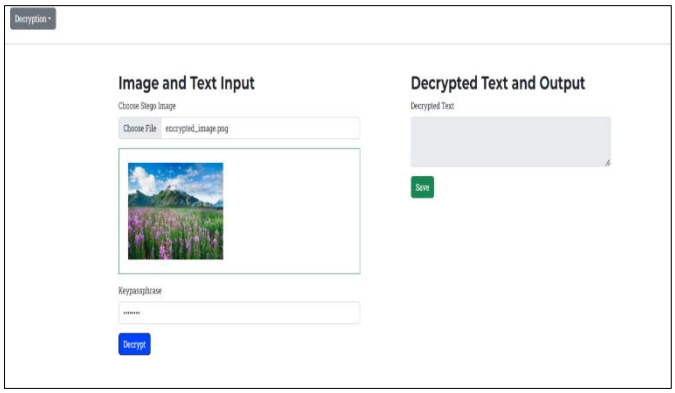

Fig -6: Decryption page layout

4.4 Decryption Results:

Upon completing the decryption process, the following results are obtained:
Decrypted Data: The original plaintext data recovered from the decrypted ciphertext.

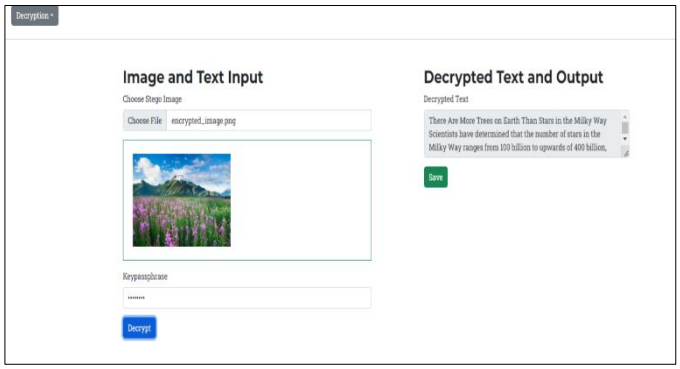

Fig -7: Decryption page Output

4.5 Discussion:

The results obtained from the encryption and decryption processes demonstrate the efficacy of the proposed system in securing data confidentiality. The encryption phase ensures that sensitive data is transformed into an unreadable format, protecting it from unauthorized access. Additionally, the steganography phase conceals the encrypted data within digital images, adding an extra layer of security. The decryption phase successfully retrieves the original plaintext data from steganographed images, providing assurance that the data remains intact and accessible only to authorized parties.

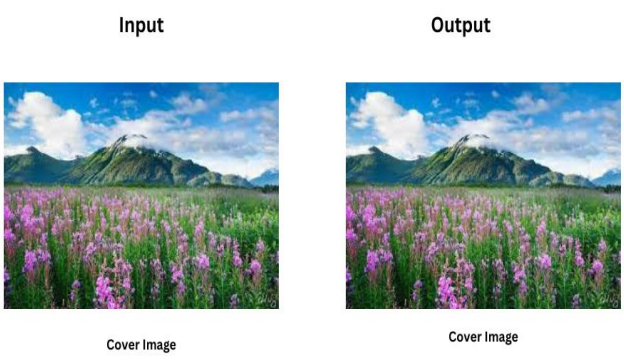

Fig -8: (a) Cover image (b) Encrypted stego image

5. CONCLUSIONS

In this project, titled "Enhancing Data Confidentiality Through Dual-Layer Cybersecurity Tool," we have successfully developed a system that combines AES cryptography algorithm with LSB image steganography algorithm to enhance data confidentiality and security. Through the integration of these two techniques, we aimed to provide a robust solution for safeguarding sensitive information from unauthorized access and interception. Our system utilizes AES encryption to secure data, ensuring that it remains unreadable to unauthorized parties. Additionally, LSB image steganography is employed to conceal the encrypted data within digital images, effectively masking its presence and reducing the risk of detection. This dual-layered approach offers a comprehensive security solution, addressing both confidentiality and stealth in data transmission and storage. Through implementation and testing, we have observed promising results in terms of security, performance, and practical applicability. The encryption and steganography processes demonstrated efficient performance, with minimal computational overhead and negligible impact on image quality. Moreover, the successful extraction and decryption of hidden data from stego images validate the reliability and robustness of our system.

ACKNOWLEDGEMENT

We would like to thank the Department of Computer Science & Engineering Lendi Institute of Engineering and Technology, Vizianagaram for helping us to carry out the work and supporting us throughout the research.

REFERENCES

1. Schneier, Bruce. "Applied Cryptography: Protocols, Algorithms, and Source Code in C." John Wiley & Sons, 1996.
2. Ferguson, Niels, and Schneier, Bruce. "Practical Cryptography." John Wiley & Sons, 2003.
3. Stallings, William. "Cryptography and Network Security: Principles and Practice." Pearson, 2016.
4. Johnson, Neil F., and Jajodia, Sushil. "Steganography: Seeing the Unseen." IEEE Computer Society Press, 1998.
5. Fridrich, Jessica, Goljan, Miroslav, and Du, Rui. "Detecting LSB steganography in color and grayscale images." IEEE Multimedia, Vol. 8, No. 4, 2001, pp. 22-28.
6. Python Imaging Library (PIL). "Pillow: Python Imaging Library." [Online]. Available: https://python-pillow.org/.
7. "A Novel Approach to Enhance Data Confidentiality using LSB Image Steganography and AES Cryptography". Authors: Anandhavelu P., Kavitha G.
   Source: 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)
8. "Image Steganography with AES Encryption Technique". Authors: Aparna Singh, Amit Kushwaha, Source: 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)
9. "A Hybrid Approach for Data Hiding using LSB Steganography and AES Cryptography". Authors: M. Kishore Kumar, T. Padmavathi, Source: 2018 International Conference on Inventive Research in Computing Applications (ICIRCA)
10. "A Hybrid Approach for Data Hiding using LSB Steganography and AES Cryptography". Authors: M. Kishore Kumar, T. Padmavathi, Source: 2018 International Conference on Inventive Research in Computing Applications (ICIRCA)