2021 International Conference on Emerging Smart Computing and Informatics (ESCI)
AISSMS Institute of Information Technology, Pune, India. Mar 5-7, 2021

Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard

Adit Pabbi
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore, India
pabbi.adit@gmail.com

Rakshit Malhotra
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore, India
raks.malhotra@gmail.com

Manikandan K
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore, India
kmanikandan@vit.ac.in

2021 International Conference on Emerging Smart Computing and Informatics (ESCI) | 978-1-7281-8519-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ESCI50559.2021.9396884

***Abstract*— Steganography is the method of hiding messages or data (plain text) by encoding them into some other data (usually images). Through this mechanism, the secured plain text message can be completely concealed from unauthorized access. Using steganography, we can hide messages by encoding it in an image and then send it to the receiving user. In our proposed method using steganography and encryption, we have implemented a mechanism to transmit a message from the sender to the receiver and increase the security of the transmission while also providing confidentiality. The receiver will receive both the encoded image and the key with why the encrypted method can be decrypted. We will be using the Least Significant Bit (LSB) method of steganography and AES encryption to achieve this.**

Keywords*— *AES, LSB, Cryptography, Steganography, Encoding, Encryption

I. INTRODUCTION

The concept of steganography involves the idea of hiding information in a file. This information can be audio, video or text, whereas cryptography is the process of encrypting the information using standard algorithms so as to not allow others to read the original information. Steganography has an added advantage compared to cryptography as the intended secret message is hidden inside an image which is not easy to notice. Attackers can't always tell if the given image has hidden data in it whereas an attacker can easily get suspicious whenever he sees an encrypted message. But the cryptography provides more security than steganography whereas steganography has more probability of not being suspicious. Thus, these two methods of security can be collaborated to form a robust tool which can do both cryptography and steganography on the information and security can be enhanced to many folds.

There are many methods to perform cryptography such as Blowfish, Data Encryption Standard (DES), Advanced Encryption Standard (AES) and so on. Also, for steganography there are many methods available such as LSB method, DCT (Discrete Cosine Transform), DWT and FFT. Considering efficiency and compatibility, AES for cryptography and LSB method for steganography is used in this paper. The cipher text formed from plain text using cryptographic algorithms is encrypted and no one can decode without knowing the key and when this cipher text is processed through steganography using an image the presence of cipher text itself is hidden and this makes it difficult to decode. Even if someone decodes the image to get the cipher text, still they need the key to decrypt it.

II. PROBLEM DEFINITION

With the spread of Internet of Things (IOT) and the transfer of data every second, the security of the communication is a challenging task. So, there is always a need to ensure security. This security can be in terms of textual, video or audio. Messages exchanged by two users can be eavesdropped and if proper security methods are not followed the privacy can be compromised. This security in terms of textual data is nowadays in form of cryptography in which the textual data is first encrypted before sending it to other user using a key. This key is known to only the participating users or one of them depending on the implementation. So, any eavesdropper cannot break this encryption unless he knows the key.

The concept of steganography hides the data into a medium so that it is not visible to the eavesdropper. If these two concepts of security are integrated and deployed as a tool, it can serve as a double security tool. The project involves a GUI based too (.exe) which takes text from user and then it encrypts using AES algorithm followed by steganography on this encrypted text using user defined image. The encoded image is saved accordingly. The text from encoded image can be retrieved using the same tool's decryption module. The decryption module involves extracting the text from image using image processing tools and techniques and this text is then decrypted using same cryptographic algorithm used for encryption. Thus, the whole process involves encryption, encoding, decoding and decryption.

III. LITERATURE SURVEY

In image steganography, we are trying to encode the text in the image using the LSB of the image and substituting it with the input data

1. The paper proposes a method to increase the security of message sent using steganography along with AES encryption.
2. In this website source, the pycrypto/pycryptodome library of python has been used and the usage of the AES methods and classes have been discussed.
3. Presents an image steganography mechanism that is able to carry audio or video and encode it. It focuses a lot on high embedding capacity and security with an decent image quality after embedding data within it. It proposes a methodology where a 'Variable Least Significant Bit' method is used to embed data, here 'n' least significant bits are used. The AES- 128 algorithm is used with 10 rounds to generate random pixel positions, each round produces 128 bits. This method is enhanced with the cipher text as the text

generated is used to generate the pixel locations, rather than the sender choosing the locations. The paper evaluates the proposed methodology on three criteria namely Time Complexity, Quality Measurement and Security. The big advantage of the paper is that even if the message is retrieved through the image, the receiver still can't access the message until they have the key to decrypt the message with.

4. Presents a refined technique for steganography in spatial domain having an acceptable embedding capacity, decent level of security and less probability of detection of visual assessment and statistical analysis techniques. The proposed technique of the paper discusses about random bits sequence and random embedding pixel location generation which uses the mathematical technique of quadratic residues. The paper uses the colour space of YCbCr along with Huffman coding. Overall, the algorithm suggested is great and has 100% embeddings to the LSBs of the cover image. The only minor disadvantage in the paper is not using the RGB color space and hence opens up scope for future research in that domain.
5. Proposes a unique technique of image steganography by using discrete wavelet transformation and singular vector decomposition techniques where the focus is on changing the HH band. The algorithm's SVD technique ensures hiding secret information without degradation in quality of the image. The experimental results for testing potency of attacks on the image suggest that the algorithm is quite resistant to image processing and geometric attacks. The PSNR, RMSE, MSSIM, FSIM and NCC values obtained in the experiments were also impressive suggesting that algorithm could be used in image steganography. There are as such no disadvantages of the algorithm apart from the complexity.
6. This paper offers a way to use the LSB method of steganography while at the same time concurrently employing RSA, AES, DES and Blowfish algorithms in order to analyse them on several factors such as histogram equalization, encryption to decryption time and signal to noise ratio. Further, in this paper the encrypted information is hidden with the usage of LSB technique. This proposed methodology presents multiple layers of data security and this makes it difficult for the intruders to find out the original data. This paper uses a unique way of the usage of mixture of cryptography with steganography to encrypt and protect the data. It similarly analyses the experimental outcome to expose the quality of the final image.

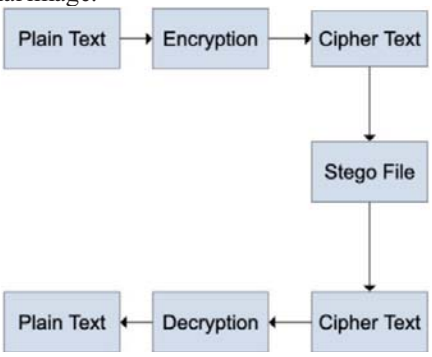

Fig. 1. Steps to encode and decode image

7. Mentions the general techniques and algorithms used in cryptography as well as how to conceal data. Data can be concealed in images in two ways - steganography and watermarking. It mentions how steganography can be divided into two parts - linguistic and technical. This can be used to encode message in audio, image and even video. On the other hand, watermarking can be robust or fragile, depending on the method used. A watermark can be used to prevent from unethical usage of important documents and files. Moreover, the paper discusses the key idea behind selecting various cover media for different usages.
8. Proposes an algorithm which is a combination of cryptography and steganography. We use multiple keys which can hide data with more security. This contributes towards a powerful tool which helps people communicate to each other and maintains confidentiality. AES is a very secure encryption method and topped with steganography it makes it more secure. Discrete Cosine Transformation (DCT) is used for encoding the message in the image

Disadvantages of existing system

- Computation time is a significant disadvantage
- The algorithm is complex and, in some cases, we may get a lot of distortion (hiding a lot of data)
- Histogram equalization and the formation of the histogram will take a lot of time and is complex.

The methods mentioned in the literature survey produce very low-quality steganography images which can be detected easily. Also, in many of these papers the data is not encrypted which does not have confidentiality. [9].

IV. PROPOSED METHODOLOGY

The proposed methodology consists of 4 modules namely: encryption, encoding, decryption and decoding. The encryption module encrypts the information using standard cryptographic technique AES (Advanced Encryption Standard) using a key. This key is known only to the encoder. The encoding module takes the cipher text formed by encryption module and user defined image as input and using steganography method of LSB the cipher text is made hidden into the image. Until this, the final output of encryption is done and the encoded steno image is formed which can be used to transmit. If there is an image which needs to be checked if it contains hidden data, decryption and decoding module is used. In decoding module, the encoded steno image is taken as input and using image processing techniques the hidden data is extracted which is nothing but the cipher text. This cipher text is input to the decryption module in which the plain text is retrieved back.

This project works on the principle of image processing, cryptographic method AES and steganography method LSB.

We also use the Mean Square Error (MSE) given by $\mathbf{MSE=1/(C\times W\times H)*(\sum_{pixels}(I_1-I_2)^2)}$ and it's inverse, the Peak Signal to Noise Ratio (PSNR) given by

$\mathbf{PSNR = -10log10*MSE}$ to analyze the impact of noise in the image.

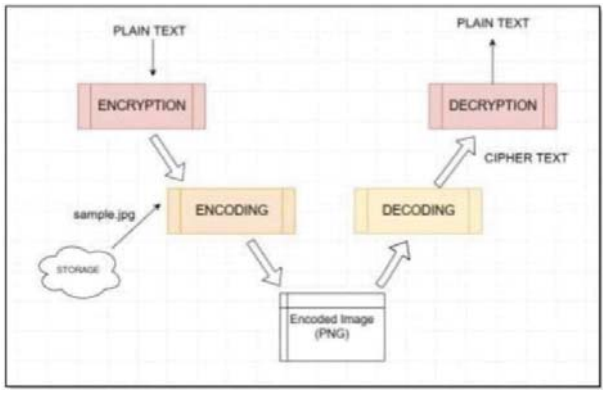

Fig. 2. Block Diagram of The Process Working Principle

V. AES SPECIFICATION

One of the most popular and widely used asymmetric and public encryption algorithm. It has a much better performance rate than the other algorithms like DES and triple DES [10]. "Some benefits of AES include -

- Symmetric Key Symmetric Block cipher
- 128-bit data, 12/192/256-bit keys

The AES algorithm is executed in CFB mode (Cipher Feedback Mode) in which the encryption process is "take the most recent cipher text block, pass it through the block cipher and then exclusive OR that with the plain text block to generate the next cipher text block."

VI. LEAST SIGNIFICANT BIT STEGANOGRAPHY

In the steganography process, firstly, the text to hide in the image is converted into image form called cipher image using python inbuilt libraries namely PIL (Python Imaging Library). The input image is divided into blue, green and red channels and for hiding the data, only red channel is disturbed and the other two channels are kept undisturbed. In the LSB method, LSB of red channel value of every pixel in the image is replaced with the pixels of the cipher image.

VII. PSEUDO CODE

Forward Pass (Encryption and Encoding):

1. Run code and start the GUI module.
2. Enter information to be hidden
3. Click Encrypt and Encode
4. Encryption: ciphertext = encrypt (text, CFB, key) key = "hello world"
5. Encoding: encodedImage = encode (ciphertext, image)

Reverse Pass (Decoding and Decryption):

1. Run code and start the GUI module.
2. Enter encoded image path
3. Click Decode and Decrypt
4. Decoding: Hiddentext = decode(encodedImage)
5. Decryption - plaintext = decrypt(hiddentext, CFB, key) key = "hello world"

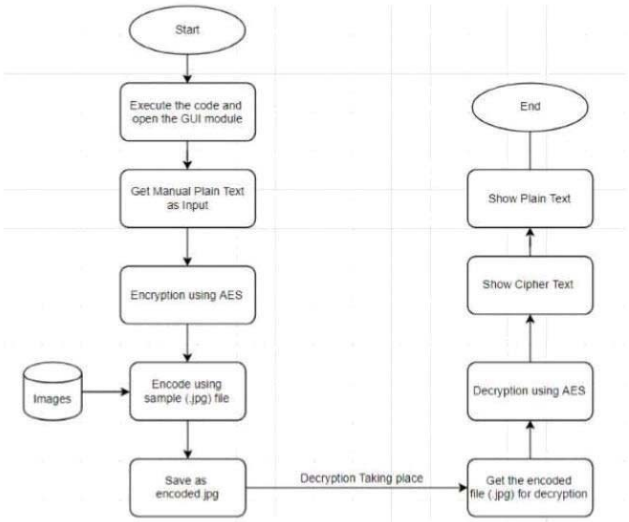

Fig. 3. Flowchart of the algorithm

Illustrations with Descriptions

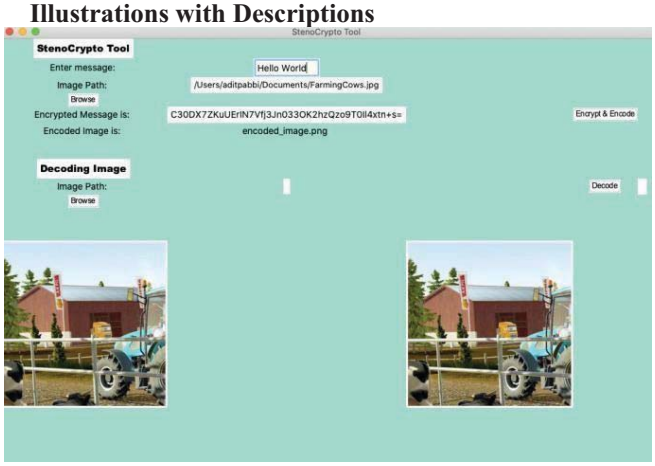

Fig. 4. Encoding the cypher text

Message = "Hello World"

Password = "The old fox"

Image = Farmingcows.jpg

First, we enter the message to be encoded into the image. We also select the image in which encoding is to be done. A cipher text of the message is generated using AES.

This cipher text is then encoded into the image using LSB steganography and a new image with the encoded text is generated.

Fig. 5. Decoding the image

Image encoded = "FarmingCowsSecret.jpg"

The path of the encoded image is taken. We decode it to generate the cipher text. They cypher text is then decrypted using the password. The message is then displayed.

VIII. RESULTS

Size of Image	Size of Cover Image	Size of message	MSE%	PSNR (dB)
1.64 MB	1.64 MB	600 bytes	0.02%	75.14 dB
1 MB	1 MB	600 bytes	0.20%	65.21 Db
500 KB	500 KB	600 bytes	0.40%	55.32 dB
45 KB	45 KB	600 bytes	0.58%	49.68 dB

Table 1 – Analysis of Steganography using MSE

We have used the Mean Square Error and Peak Signal to Noise Ratio (PSNR) to analyze the distortion and noise across the same image of different sizes. As it can be seen, the PSNR decreases as the image size reduces but is still quite significant, which indicates that the naked eye won't be able to differentiate a cover image from the real one.

We have successfully encrypted the message using AES and hid in the image using Steganography and the receiver were also able to decrypt the image and get the cipher text.

With the ciphertext, the user uses AES decryption and is able to get the plain text.

IX. CONCLUSION AND FUTURE WORK

We conclude that, using both cryptography and steganography enhances the security and also the complexity which restricts the attacker from attacking the system. This system can be implemented in places where security cannot be compromised and they cannot afford to be suspicious in the eyes of the attacker.

ACKNOWLEDGMENT

We would like to thank our supervisor and corresponding author, Dr Manikandan K for his help and guidance in the implementation of this project.

We would also like to thank our college Vellore Institute of Technology, Vellore for giving us the resources to implement and run this project.

REFERENCES

[1] Utsav Sheth and Shiva Saxena, "Image Steganography Using AES Encryption and Least Significant Nibble", International Conference on Communication and Signal Processing, April 6-8, 2016, India

[2] Pycrypto dome library source https://www.dlitz.net/software/pycrypto/api/current/Crypto.Cipher.AES-module.html

[3] C. Lalengmawia and A. Bhattacharya "Image Steganography using Advanced Encryption Standard for implantation of Audio/Video Data", 2016 Fifth International Conference On Recent Trends In Information Technology

[4] Mark Rennel D. Molato, Bobby D. Gerardo, and Ruji P. Medina. 2018. "Secured Data Hiding and Sharing using Improved LSB-based Image Steganography Technique". In Proceedings of the 4th International Conference on Industrial and Business Engineering (ICIBE' 18). Association for Computing Machinery, New York, NY, USA, 238–243.

[5] Mansi S. Subhedar and Vijay H. Mankar. 2014. "High-Capacity Image Steganography based on Discrete Wavelet Transform and Singular Value Decomposition". In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '14). Association for Computing Machinery, New York, NY, USA, Article 63, 1–7.

[6] Masumeh Damrudi and Kamal Jadidy Aval. 2019. "Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish." International Journal of Engineering and Advanced Technology (IJEAT). ISSN: 2249 – 8958, Volume-8, Issue-6S3, September 2019

[7] Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial and Brendan Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research", Neurocomputing, Volume 335,2019, Pages 299- 326, ISSN 0925-2312

[8] Dipti, K. S. and Neha, B. 2010. "Proposed System for Data Hiding Using Cryptography and Steganography". International Journal of Computer Applications. 8(9), pp. 7-10. Retrieved 14th August, 2012

[9] Raphael, A. J., and Sundaram, V. 2011. "Cryptography and Steganography - A Survey". International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.

[10] A.A. Tamimi, "Performance Analysis of Data Encryption Algorithms. Retrieved October 1, 2008 From http://www.cs.wustl.edu/~jain/cse56706/ftp/encrypt ion_perf/index.ht