ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019
7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)
19th-20th March 2019
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

# Obscuring the Message in Digital Image Using Steganography

Deepa.K[1], Kirthika.B[2], Lavanya.R[3], Kesavarthini.R[4]

Professor, Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India[1]

U.G. Student, Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India[2,3,4]

**ABSTRACT**: In the modern world of digital communication, many advanced techniques have been developing which gives rises to the several forms of attacks on data and information from the intruders. To overcome these attacks, important messages has to be sent secretly through color images. In this paper, Steganography technique is used which hides secret messages within digital image without modifying the original data. The secret messages are encrypted using Advanced Encryption Standard (AES) Algorithm, then the encrypted message is concealed in the color image using LSB technique. The original image is identical to the image containing secret message.

**KEYWORDS**: Steganography, Stego image, AES, LSB, Encryption

## I. INTRODUCTION

In rapid growing modern technological world the communication of the data being less secured due to the potential computer users are increasing. Today the internet has become a necessity. Information in the form of the texts, images, videos has become the common media sharing sources through internet. Due to the higher usage of internet the attention for the security level has been reduced. Therefore, today many technologies are reinforced to maintain data security and overcome these attacks from cybercrime attacks. In that way, Steganography is one of the most famous technique which works to hide secret data into digital media like images, video, audio, etc to secure the communication.

[1]Steganography is the method of concealing the secret data into non-secret file in order to avoid detection. Steganography word is the origin of two Greek words Stegos means protected or covered and graphos means writing. This technique literally performs the embedding of one source into another. In image Steganography, we embed the text into an image over an image. The image which is used as the source is the cover image and the information is embedded into it, the image becomes Stego image. The information which has been inserted in the image is not suspicious to the intruders.

This paper is organized as follows. Section II describes the flow chart and its description. Section III presents the AES Algorithm. Section IV presents about the LSB technique and Section V presents experimental results showing the comparison of Original Image and the Stego Image. Finally, Section V presents conclusion.

## II. RELATED WORK

The main idea of the proposed paper is to provide the secure communication by using the Steganography technique. The secret message which needs to be transmitted from sender to the receiver should not to be attacked by any of the Trojans, hackers, intruders, etc. The image is encrypted by using Advanced Encryption Algorithm (AES) and then the encrypted message is inserted into the Image by using the Least Significant Bit (LSB) technique. The combination of these techniques will embed the message in the color image.

Advanced Encryption Standard (AES) is the most popular and symmetric algorithm which is widely used in the recent technologies. This algorithm uses same key for both encryption and decryption process. The key could be

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

identical or may have simple transformation within the two keys. Key size or key length is the number of bits used for encryption process. The computations are performed on bytes rather than bits.
[3]The number of rounds in encryption and decryption process of the AES depends on the length of the key. Our project is based on some of the following factors and they are illustrated as follows,

1. **Input Image:** The image is selected to hide the secret information. We selected the information in a text file and the length of the files are depends upon the image quality.
2. **Image Quality Selection:** If the quality of the image is more, then the data hidden will be less and vice versa.
3. **AES Encryption:** The Secret data has been encrypted by using this technique and it provides a double layer of security check. Suppose if the hacker decodes the text in image, the decoding of AES encryption information cannot be able to encrypt.
4. **LSB Algorithm:** This technique is used to hide the information on the lower bits of the image. It is an efficient technique and vast amount of data can be hidden.
5. **Encoded and Encrypted Image**: Now the image is ready to send to the receiver but it cannot be able to know the data hidden in the image unless a receiver has a secret key.

By applying all these steps, a data can be encrypted into the image and after receiving the data, it can be decrypted. Thus the hackers will not be able to find the information which is hidden.

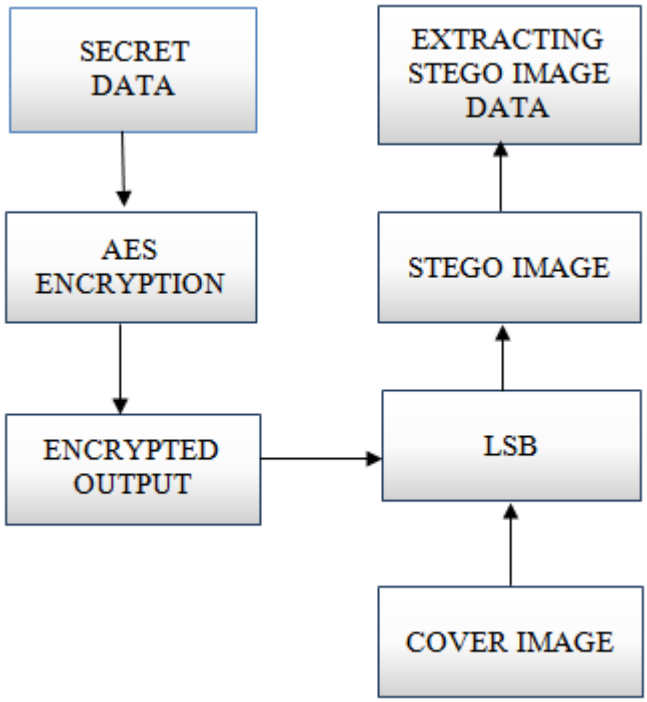


*Fig 1. Flow chart of Steganography using AES and LSB technique*

## III.AES ALGORITHM

AES is mainly aimed at providing secure communication by encrypting and decrypting process. In encryption, there are four sub process which are Sub Bytes, Shift Rows, Mix Columns and Add Round Key. They are explained as follows;

- **Sub Bytes-** 16 bytes128 bits) are assigned as 4 rows and 4 columns which are substituted by S box as in Fig.2(a).

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

- **Shift Rows**-In each rows the shifting of positions has been varied. It results in new matrix with 16 bytes as in Fig.2(b).
- **Mix Columns**-It replaces the original columns with new 4 bytes and results in 16 new bytes of matrix as in Fig.2(c).
- **Add Round Key**-It is performed using XOR operation and results as cipher text in last round as in fig.2(d).

In decryption, the process is reverse order of an encryption

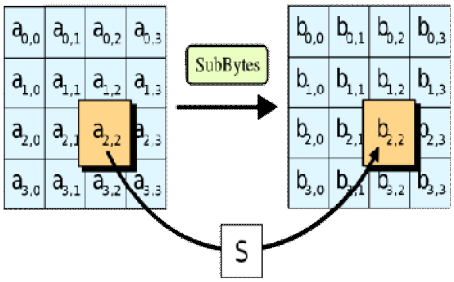


*Fig.2 (a) Sub Bytes*

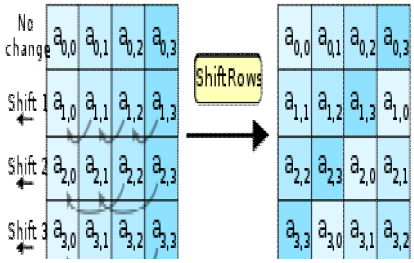


*Fig.2 (b) Shift Rows*

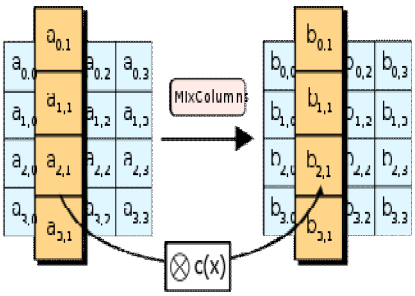


*Fig.2 (c) Mix Columns*

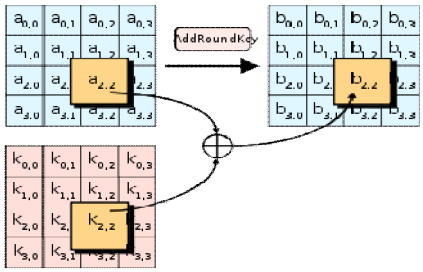


*Fig.2 (d) Add Round Key*

## IV.LSB TECHNIQUE

[4]LSB Technique is used to insert the encrypted message in a color image. Each pixel in image form the combination of RGB pixel which is represented by 3 bytes in 24-bits. In this technique we can embed 3 bit data in each pixel of 24-bit image and replaces those LSB's with 3 message bits Instead of replacing all 3 LSBs of a pixel it is replacing only one bit of a single color component. This can be red, green or blue color component from the pixel.

For example, [5]If a letter 'a' is to be embedded in image which is represented as **01100001** in binary the first bit 0 is embedded in only one color component of the pixel. It can be chose in any color as per component either Red, Blue or Green. Consider there are 8 adjacent pixels (24bytes) with RGB encoding.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019
7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)
19th-20th March 2019
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

| | | |
|---|---|---|
| 10001101 | 01110110 | 11101011 |
| 11010010 | 10000011 | 00110011 |
| 10111010 | 11101011 | 10000001 |
| 10001101 | 01110110 | 11101011 |
| 11010010 | 10000011 | 00110011 |
| 10111010 | 11101011 | 10000001 |
| 10001101 | 01110110 | 11101011 |
| 11010010 | 10000011 | 00110011 |

*Fig.3 (a) Original Cover Image Grid*

| | | |
|---|---|---|
| 10001101 | 01110110 | 11101010 |
| 11010010 | 10000011 | 00110011 |
| 10111010 | 11101011 | 10000001 |
| 10001101 | 01110110 | 11101010 |
| 11010010 | 10000011 | 00110010 |
| 10111010 | 11101011 | 10000000 |
| 10001101 | 01110110 | 11101010 |
| 11010010 | 10000011 | 00110011 |

*Fig.3 (b) Modified Image Grid*

Each bit of each character is embedded in last LSB of each pixel of cover image. Since only each pixel's last bit of cover image gets changed, this method produces modified image which contains secret data that is totally indistinguishable from the original image. This technique can be applied for the bitmap and jpeg format images.

## V.MESSAGE CONCEALMENT IN IMAGE

After encryption of the message using AES algorithm, [2]the encrypted text is converted into ASCII equivalent form which then converted to binary data format. For example, if the encrypted letter is "k" its equivalent ASCII value is 107 and binary equivalent is 01101011. This binary value is embedded in an image by using the embedded using the LSB technique.

- Firstly, the image pixels are iterated. Extracts the RGB values and separates each value in a separate integer in every iteration.
- In those RGB values make the LSB values to 0. Only these bits are used in concealing the characters.
- Fetch the current character and convert it to the binary value. These binary values are hided in its 8 bits in R1, G1, B1, R2, G2, B2, R3, G3, B3, where the numbers refer to the number of the pixels. The entire text is gets iteratively concealed in the LSB.
- After processing the 8 bits of that particular character, then move to the next character, and reiterate the same process till the whole message is concealed.
- The encrypted message is concealed in LSB portion of the image based on the length of the message. Therefore, there must be an indicator to indicate the end of message. The indicator is basically 8 sequentially zeros and this is used in the message extraction from the image phase.

## VI.EXPERIMENTAL RESULTS

The Fig.4 (a) is original image and the Fig.4 (b) is a stego image where it has a secret data within it. Stego image have no variation from original image because the quality of stego image remains same as the original image. By analysing the properties of the image from the Fig.4 (c), it is concluded that the image has a secret data in it. The Stego-image will be same as the original image after performing LSB concealment. The modification in the original image (cover image) is not noticeable on the stego-image to the human eye. Even the size of the original image is not changed.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 8, Special Issue 1, March 2019

7th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '19)

19th-20th March 2019

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

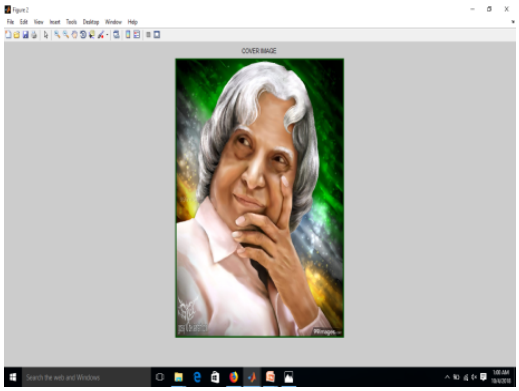

*Fig.4 (a) Original Image*

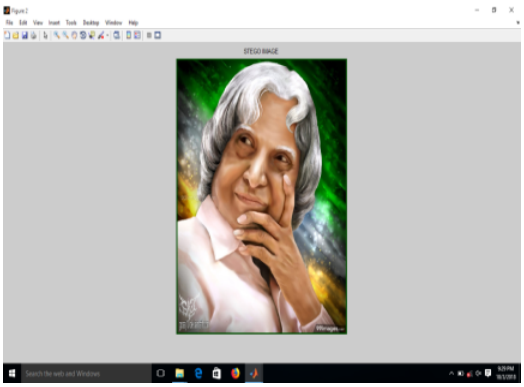

*Fig.4 (b) Stego Image*

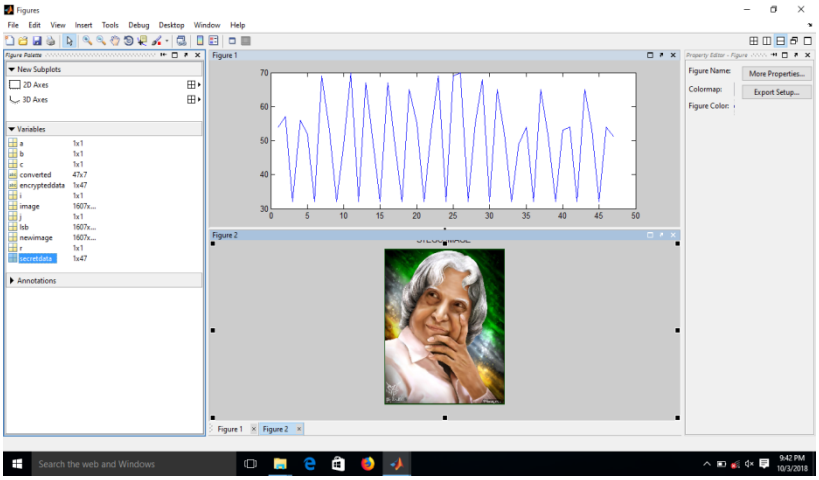

*Fig.4 (c) Secret data embedded in cover image*

## VII.CONCLUSION

Experimental results show that the image quality remains same even after embedding the data. The concealment of the data into the image will not seek attention of intruders since original and stego image remains same. By using AES and LSB techniques, the data is secure it doesn't allow any suspicious to the intruders which to the secure data in transmission over an exposed channel.

## REFERENCES

[1]Nurhayati, Syukri Sayyid Ahmad, "Steganography for inserting message on digital image using Least Significant Bit and AES Cryptography Algorithm", in 4th International Conference on Cyber and IT service Management, 2016.
[2]Arun Kumar Singh,Juhi Singh,Dr.Harsh Vikaram Singh, "Steganography in images using LSB technique", International Journal of latest trends in Engineering and Technology (IJLTET), Volume 5 issue 1, January 2015.
[3]Roshini Padate, Aamna Patel, "Image encryption and decryption using AES algorithm" in International Journal of Electronics and communication engineering and technology (IJECET), Volume 6 issue 1, June 2015.
[4]Unik Lokhande, "An efficient way of using LSB Steganography in images along with Cryptography" International Journal of Computer Applications, Volume 88, no.12, Februray 2014.
[5]Mr.Alok Sharma, Nidhi Sharma, Dr.Ankit Kumar, "A New Algorithm to Secure Image Steganography File", 7th International Conference on cloud computing data science and Engineering Conference,2017.