LSB BASED TEXT AND IMAGE STEGANOGRAPHY USING AES ALGORITHM

Priya Paresh Bandekar[1] and Suguna G C[2]
[1]Student of ECE Department, JSSATE, Bangalore
priyabandekar1234@gmail.com
[2]Assistant Professor of ECE Department, JSSATE, Bangalore
Sgc.mtech2006@gmail.com

Abstract-

The steganography is the art of hiding data in another data. Secret information like messages, images, audio and video can be hidden inside the cover image. The main objective is to hide the secret message or image inside the image using Least Significant Bit (LSB) technique. To protect and provide security for the hidden message or image, Advanced Encryption Standard (AES) Algorithm is used. Various image formats with different text length or image size are compared. Efficiency of algorithm is estimated by Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) where higher PSNR value gives the high-quality image. Steganography plays an important role in applications like medical, military, OTP (One Time Password), copyright etc.

Keywords- Image steganography, LSB, Advanced Encryption Standard, PSNR Ratio, MSE, OTP.

I. INTRODUCTION

Steganography becomes of greater significance in the digital era as more people are joining cyber space revolution. Computer network requires special means of security as the number of data being exchanged on the internet is increasing. Therefore, confidentiality and data integrity plays a major role to protect against unauthorized access. Information hiding is an emerging research area in modern communication. This includes applications such as watermarking, fingerprinting, copyright protection and steganography.

In ancient time, the use of invisible ink or shaving the messengers head and then sending the person one's the hair grows or wooden wax was used as a medium in order to pass the secret communication from sender to receiver. The problem with this way of communication was the information was not secured. With the advancement in the technology, internet came into existence. As a result all the information transfer took place over the web. In the modern era, the word steganography means to hide the secret data in a file so that the third person is unaware of the existing hidden data into the image. The hidden secret information can be in two insertion domains: spatial domain and frequency domain. Our main focus is in the spatial domain [10] because the changes in the cover image are indistinguishable by the human eye. The spatial domain performs the dissimilation in the bits of the pixel of the original image. LSB (Least Significant Bit) technique is one of the spatial domain techniques. In LSB each of the bit of the data i.e. the character or the image are placed in the least significant bit of the cover image so that the distortions brought by the insertion process remain imperceptible by the human eye.

In our work we study about the LSB technique (LSB) i.e. embedding the secret data into the cover image [9] and in order to protect and provide security for the stego-image AES (Advanced Encryption Standard) algorithm is used [1][2]. We take different images of various formats and try to hide the secret data of varied length into the cover image. Then PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) between the original and the encrypted image is estimated. PSNR, MSE and histogram is also plotted.

The paper is organized as following: section II presents LSB substitution and AES algorithms. Section III presents proposed works LSB with AES algorithm. Section IV presents experimental results. Section V presents general conclusion.

II. METHODS

A. Least Significant Bit

Least Significant Bit is one of the spatial domain techniques where each bit if the text or the image is substituted from the least significant bit of the original image. It is simple and easy to implement. The specialty of its existence in spatial domain is because the human eye cannot distinguish between the original and encrypted image [4]. LSB can be extended up to 4-bits or 2-bits out of 8-bits, but it may cause distortion in an image due to change in the intensity of an image. LSB substitution comprises of

1. LSB Encoder
2. LSB Decoder

LSB technique has become the basis of many techniques that hide the secret data within the carrier data. First section explains about the encoding process where the secret data is hided and next section explains about the decoding process where the data gets extracted [5].

LSB Encoder

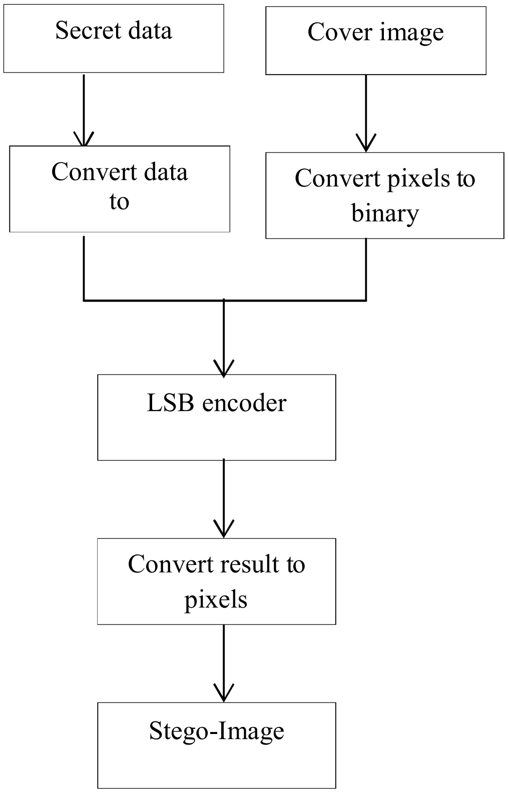


Figure 1: LSB encoder

1. Input the secret data i.e. text or the image which needs to be hidden.
2. Input the cover (original) image of size [256 256].
3. Convert the secret data i.e. asci value of each text or pixel value in case of image into binary representation.
4. Convert the pixel value of cover image into binary representation.
5. Apply LSB encoder; function is to hide each bit of text or image into the least significant bit of each 8 pixel value of cover image.
6. The resultant output is converted back to pixel values to get the stego-image.

LSB Decoder

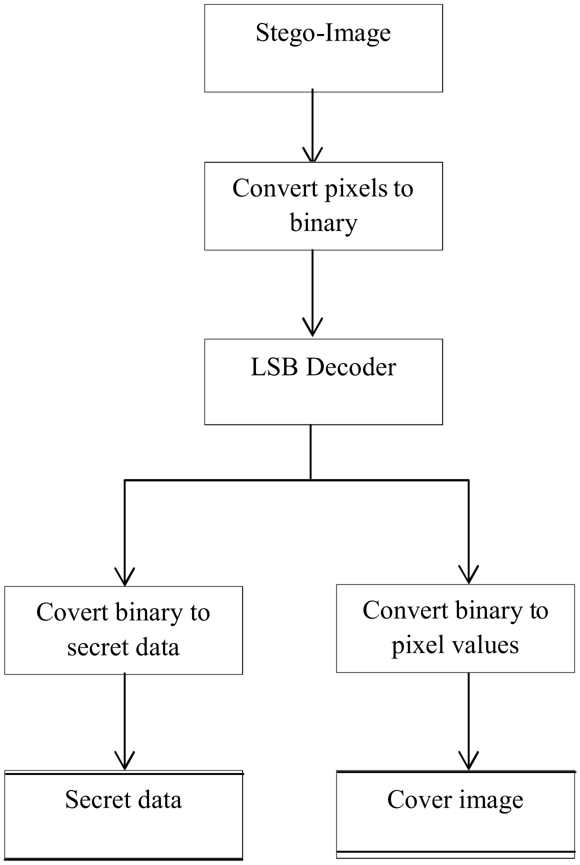


Figure 2: LSB Decoder

1. Input the stego image.
2. Convert the pixel value to binary representation.
3. Apply LSB decoder; function is to retrieve the secret data back from the stego-image.
4. The secret data and the cover image are separated together to get the desired output.

B. AES (Advanced Encryption Standard)

The AES algorithm is the symmetric algorithm that is secure enough to provide security for confidential data operating on plaintext of 128-bit with variable key length of 128, 192 and 256-bit [3]. The number of rounds performed is 10, 12 and 14 respectively. AES is one of the strongest algorithms until now and we can use only one key at the sender and receiver side, hence the privacy made by the key is secured.

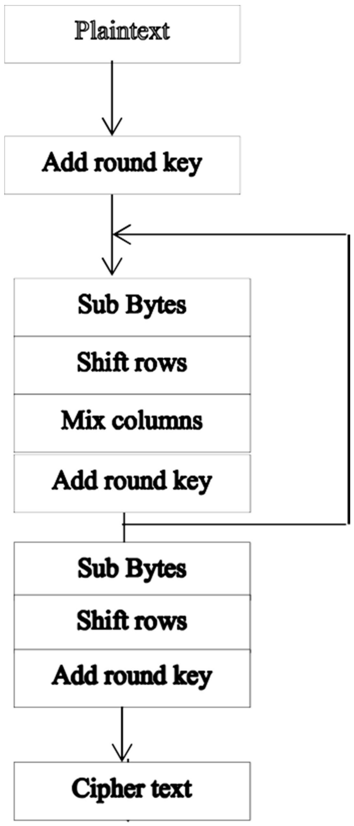


Figure 3: AES Encryption Algorithm

AES ENCRYPTION

All operations in AES are byte oriented. 128 bit plaintext is arranged in 4x4 matrixes with 16bytes. Substitute byte, shift rows, mix columns and add round key are the main steps in AES encryption [7].

a) Sub Bytes Transformation
Sub byte is substitute byte where each byte from the cipher text is substituted from the standard look up table of s-box which contains 256 elements. S-box is shown in fig. First hexadecimal values in byte indicate row index and second hexadecimal value indicate column index.

b) Shift Rows Transformation
In shift row transformation, the rows of the matrix are circularly left shifted. Row 0is kept constant; Row 1 is left shifted by 1 byte; Row 2 is shifted by 2 byte and finally last row by 3 byte.

c) Mix Column Transformation
Each column in the new formed matrix is multiplied with each column of the predefined matrix.

d) Add Round Key
The resultant matrix is xor-ed with the expanded key generated from the initial key.

AES DECRYPTION

Decryption is just the opposite of encryption i.e. the cipher text is converted back to the plain text. Inverse substitute byte, inverse mix column, inverse shift rows and inverse s-box takes place.

a) Inverse Sub Byte Transformation
Each byte from the matrix is substituted with the inverse s-box table to get the new matrix.

b) Inverse Shift Rows Transformation
The row of the matrix is circularly right shifted.

c) Inverse Mix Columns Transformation
Function opposite to that of mix column transformation.

d) Inverse Add Round Key Transformation
The round keys should be selected in a reverse order and Xor-ed with the state matrix.

III. LSB combined with AES Algorithm

Our approach is to provide security for the secret information hidden inside the cover image performed through LSB technique [6] with the help of AES algorithm. The first step is to read the secret data and the cover image. The next step is to hide the data into the cover image which is done with the help of LSB encoder. To protect the data from the intruder the resultant stego-image is given to AES encryption where each of the pixels get scrambled .To get back the stego-image AES decryption is done and the output of this is provided to LSB decoder where the hidden data is retrieved finally [8].

General Block Diagram:

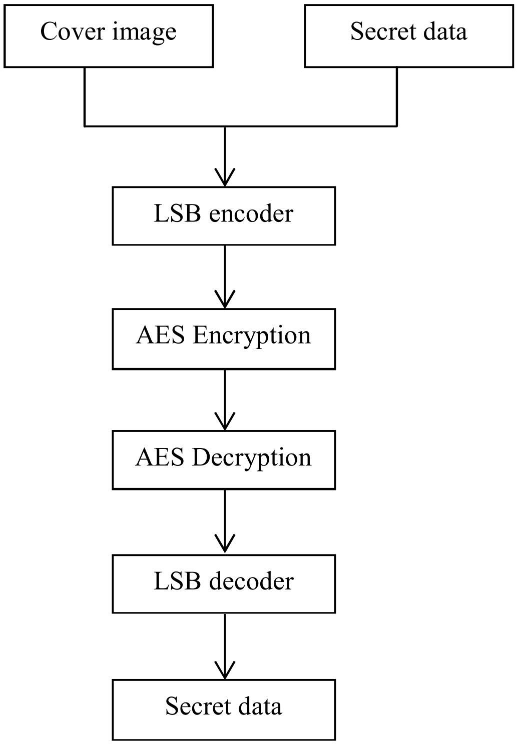


Figure 4: LSB combined with AES algorithm

1) Read the input cover image of size [256 256].
2) Read the secret data i.e. text or the image.
3) Apply LSB encoder where the bits of the secret data are hidden into the least significant bit of the pixel value of the cover image.
4) The resultant stego-image is given to AES encryption in order to provide security for the hidden data.
5) The function of the AES decryption is to get back the stego image in order to retrieve back the data.
6) The LSB decoder finds each of the data which was embedded in the cover image and the resultant is the secret data.

IV. EXPERIMENTAL RESULTS

In this work, we used LSB technique in order to hide the secret data i.e. text or image using LSB technique. Further in order to provide and protect the data AES algorithm is applied with the maximum key length of 128 bit. Image steganography is implemented in MATLAB software.

Images of various sizes are used and further resized the image into 256x256 pixel values. We choose image of type TIFF format because the size of the stego-image is no change in comparison with the original image [4]. TIFF format is lossless compression for archiving images.

Using the above two algorithms, we have hidden the text or the image inside the cover image and is also successful in retrieving back the hidden data. We compare the various images with the same text length and also with varied text length and also same in case of secret image where the size is less than or equal to 80x80.Estimation of PSNR ratio, MSE and histogram is plotted.

TEXT INSIDE IMAGE

8-bit length

Image(256x256).tiff	PSNR RATIO(dB)	MSE
Boat	52.3728553	0.38
Barbara	53.1204016	0.32
Cameraman	53.2416592	0.31
Couple	54.9964493	0.21
Fingerprint	55.380342	0.19
Lena	52.8258176	0.34
Mona Lisa	48.5456915	0.91
Stairways	53.3657362	0.30
Tower	52.9426629	0.33
Cat	52.8250.63	0.34

Table 1: Text inside Image for 8-bit text length

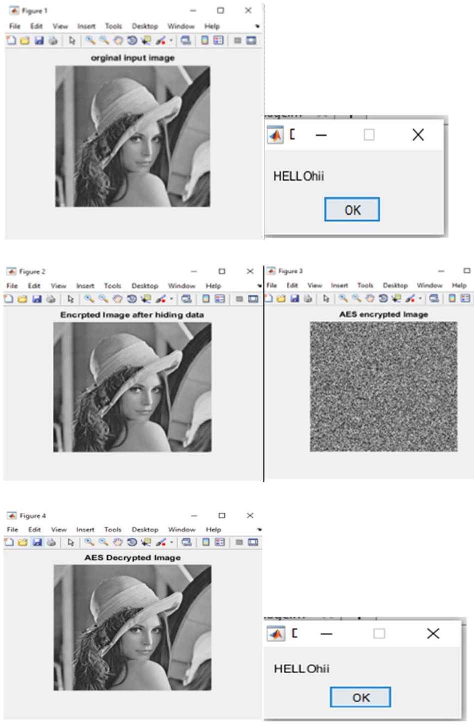
Table 1 depicts hiding of text inside image of text length of 8-bit long. It infers that it has different PSNR and MSE for different images and as the PSNR ratio increases, the MSE decreases indicating good quality of the image.

256-bit length

Image(256x256).tiff	PSNR RATIO(dB)	MSE
Boat	52.2368628	0.39
Barbara	52.9530097	0.33
Cameraman	53.0662400	0.32
Couple	5407240130	0.22
Fingerprint	55.0917353	0.20
Lena	52.6709765	0.35
Mona Lisa	48.5088875	0.92
Stairways	53.1816601	0.32
Tower	52.7823693	0.35
Cat	52.6649955	0.35

Table 2: Text inside Image for 256-bit text length

Table 2 gives the hiding of text inside the original cover image of text length of 256 bit long.



HELLOhii

HELLOhii

Figure 5: Text inside Image

Figure 5 infers hiding of Text inside image using LSB encoder, encrypting the stego image using AES encryption, decryption in order to provide security and finally retrieving back the hidden text from the stego image using LSB decoder.

PSNR AND MSE PLOT

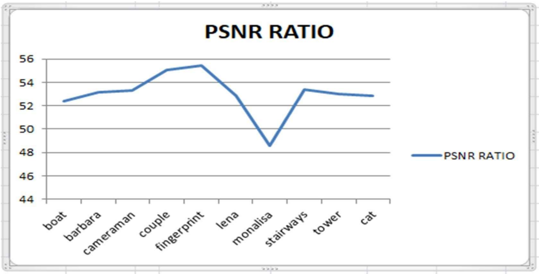


Figure 6: PSNR RATIO for 8-bit text length

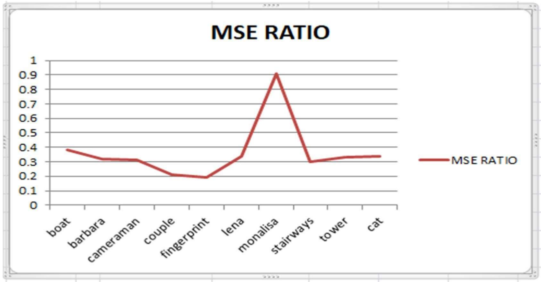


Figure 7: MSE RATIO for 8-bit text length

Figure 6, 7 shows the PSNR ratio and MSE for 8 –bit text length which are inversely proportional to one another.

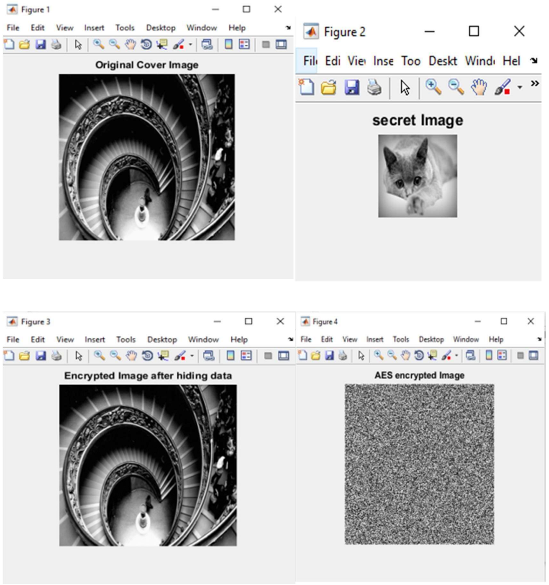


Figure 1
File Edit View Insert Tools Desktop Window Help
Original Cover Image
Figure 2
Fil Edi Vie Inse Too Deskt Wind Hel
secret Image
Figure 3
Encrypted Image after hiding data
Figure 4
AES encrypted Image

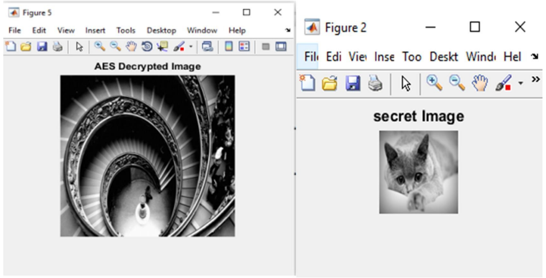


Figure 5
File Edit View Insert Tools Desktop Window Help
AES Decrypted Image
Figure 2
Fil Edi Vie Inse Too Deskt Wind Hel
secret Image

Figure 8: Image inside Image

Figure 8 shows hiding of Image inside Image using LSB encoder, encrypting the stego image using AES encryption, decryption in order to provide security and finally retrieving back the hidden image from the stego image using LSB decoder.

IMAGE INSIDE IMAGE

Original image(.tiff)	Secret image(.tiff)	Size(<=[80 80])	PSNR ratio	MSE
Barbara	boat	[45 45]	56.6324644	0.12
		[60 60]	54.1947196	0.22
		[80 80]	51.6948071	0.39
cat	cameraman	[45 45]	51.6723418	0.39
		[60 60]	54.1668937	0.22
		[80 80]	56.6827528	0.12
stairways	cat	[45 45]	51.6403766	0.39
		[60 60]	54.1798771	0.22
		[80 80]	56.6361893	0.12
tower	stairways	[45 45]	51.6614912	0.39
		[60 60]	54.1847180	0.22
		[80 80]	56.6666400	0.12
Lena	Mona Lisa	[45 45]	51.6767576	0.39
		[60 60]	54.1690046	0.22
		[80 80]	55.6144174	0.13

Table 3: Image inside Image

Table 3 depicts hiding of secret image of size <=80x80 into the original image of size 256x256 and calculating the PSNR ratio and MSE for different images.

PSNR AND MSE PLOT

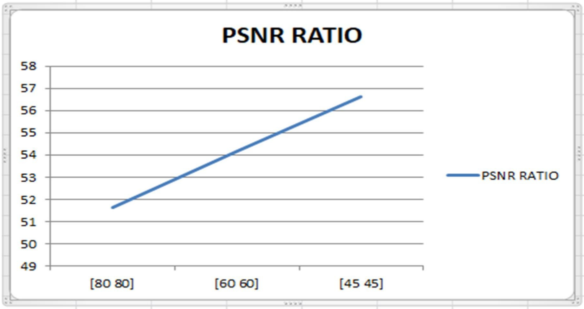


Figure 9: PSNR RATIO for Image inside Image

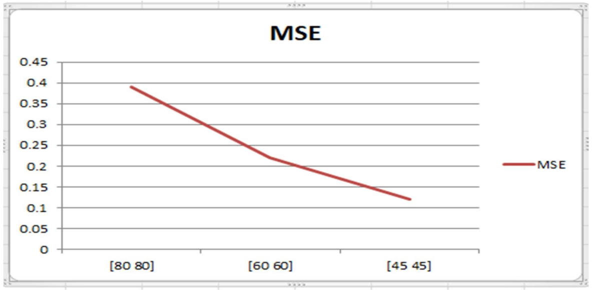


Figure 10: MSE RATIO for Image inside Image

Figure 9, 10 shows PSNR ratio and MSE for image inside image which are proportional to each other from the experimental result.

V. CONCLUSION

In this work, we hide the secret data into the cover image using LSB technique where the maximum number of characters embedded is 8192 characters and the secret image size is less or equal to 80x80. Hence in order to provide security for our hidden information we apply AES algorithm with key length of 128 bit which is one of the symmetric algorithm recommended by NIST and provide more security than other algorithms.

Based on our implementation of this algorithm in MATLAB environment, we compared PSNR and MSE for different images and plotted graph respectively. On plotting the graph, we studied that both PSNR and MSE are inversely proportional to each other. Lower value of MSE tells us that the error between original and encrypted image is less and higher PSNR gives that the quality of reconstructed image is better. The PSNR ratio lies in the range 45-70 dB and MSE in range of 0-1.

In this work, we hide text or image in another image. Further study about hiding audio and video inside an image will be done soon. The key length used in AES can be increased.

REFERENCES

1. NIST, “Advanced Encryption Standard,” http://csrc.nist.gov/ publications/fips/fips197/fips-197.pdf, 2001 (accessed March 24, 2017).

2. Gurpreet Singh and Supriya proposed a paper “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for information security”.

3. Qi Zang and Qunding proposed paper by name “Digital Image Encryption based on Advanced Encryption Standard [AES] algorithm”,2015 fifth international conference on instrumentation and measurement, computer, communication and control.

4. Harpreet Kaur and Ajay Kakkar proposed a paper “Comparison of different image formats using LSB steganography”, 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC).

5. S.M Masud Karim, Md.Saifur Rahman, Md.Ismail Hossain presented a paper “A new approach for LSB based image steganography using secrete key”,14th international conference on computer and information technology, December,2011.

6. Aman Arora, Manish Pratap Singh, Prateek Thakral, Naveen Jarwal proposed a paper by name “Image steganography using Enhanced LSB substitution technique”,2016 fourth international conference on Parallel, Distributed and Grid Computing.

7. Priya Deshmukh presented a paper on “An image encryption and decryption using AES algorithm”, International Journal of Scientific & Engineering Research, Volume 7, Issue 2, February-2016.

8. Z. Y. Al-Omari and A. T. Al-Taani, “Secure LSB steganography for coloured images using character-colour mapping,” 2017 8th International Conference on Information and Communication Systems (ICICS), 2017, pp. 104-110.

9. D. Samidha and D. Agrawal, “Random image steganography in spatial domain,” 2013 International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013, pp. 1-3.

10. Ali K. Hmood B. B. Zaindan, “an overview on hiding information techniques in images,” journal of applied sciences, vil. 10, no. 18, 2010.