International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 03 – Issue 06 || June 2018 || PP. 18-27

Digital Image Steganography Using Modified LSB and AES Cryptography

Subhash Panwar[a], Shreenidhi Damani[b], Mukesh Kumar[c]
[a]*Department of IT, Assistant Professor,Govt. Engg. College, Bikaner, 334004,India*
[b]*Department of CSE, PG Student, Govt. Engg. College, Bikaner, 334004,India*
[c]*Department of CSE, UG Student, Govt. Engg. College, Bikaner, 334004,India*

Abstract: With the rapid growth of technology in the area of Theoretical Computer Science, secrecy of data has been compromised and cyber-crimes are increasing at an alarming rate. This calls for a method to secure the digital messages being sent over the internet. This paper discusses about a concept on hiding the confidential data in an image which is called as Image Steganography. In addition, it uses a technique known as Cryptography to improve the strength of security. Steganography hides the data and makes it difficult to understand whether it actually exists or not. Image Steganography specifically refers to hiding the data inside a cover image. Cryptography means to modify the data in such a way that its meaning is unidentifiable. Steganography when used alone does not guarantee the protection of data, so it is used along with Cryptography. Steganography has its applications in fields which require a higher level of security such as online banking, defence and intelligence etc. Image Steganography is achieved using Modified LSB. Modified LSB uses a certain condition to replace the bits of the confidential data at the least significant bit position of the pixels in the image. Cryptography is achieved using AES. Advanced Encryption Standard AES is used to encrypt the secret data. In this way, Steganography and Cryptography when used together ensures enhanced security of digital messages.

Keywords: Advanced Encryption Standard, AES, Cryptography, Image Steganography, Least Significant Bit, LSB, Steganography.

1. Introduction

In today's modern scenario, the useful data is stored and shared via digital media. It requires the media as well as the communication channels to be safe enough to ensure security of the information. A technique known as Steganography is used for this purpose. Steganography is a word derived from Greek which means "covered writing". It hides the fact whether the data is alive or not, which is hidden inside a carrier medium which can either be text, image, audio or video. When a person sees the cover object, he cannot identify the existence of any information inside the cover object. The cover object, is thus, sent over a network to the desired destination and the intended recipient receives it [1]. When the pixels of an image hide the confidential data within themselves, it is referred to as Image Steganography.

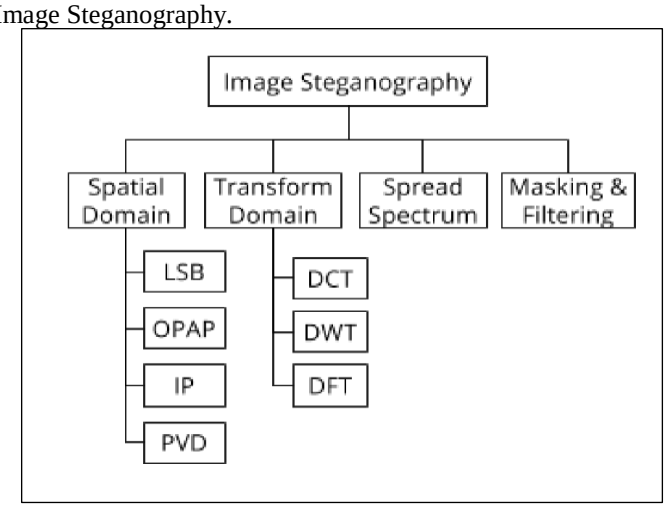


Fig.1. Types of Image Steganography [2]

Digital images are stored in 8-bit or 24-bit formats. A 24-bit image is better at hiding information. The three primary colours: red, green, and blue make for all the variations and shades in the colours in the pixel. Each primary colour is represented by 1 byte; 3 bytes per pixel are used in 24-bit images to represent a colour

value. Hexadecimal, decimal, and binary forms are used as representation for 3 bytes. A white colour has hexadecimal value FFFFFF: representing FF for red, green and blue respectively. Its binary value is 11111111, 11111111, 11111111, and decimal value is 255, 255, 255 which are the three bytes making up white [3]. In this way, individual bits from the three bytes are used to hide the secret information. Various algorithms can be used to select which bits to be replaced with the secret data. The secret data to be hidden is subject to various transformations so that the message is unintelligible to intruders. This technique is known as Cryptography.
Cryptography is a word derived from Greek which means "secret writing". Cryptography is used as a security enhancement to Steganography. Cryptography is concerned with the alteration in the structure of the message. It converts the secret data into a non readable format, which can only be deciphered by the intended receiver.

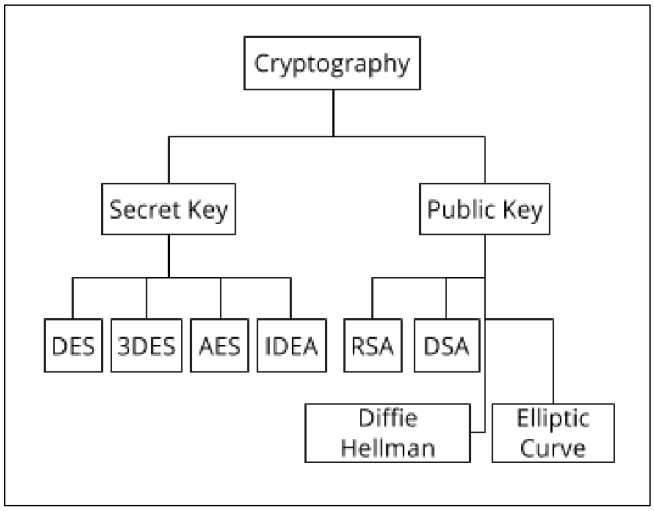


Fig.2. Cryptography and its types[4].

1.1 Classical LSB Technique

The technique for classical least significant bit implies replacing LSBs of cover image with the bits of the concealed message and manipulating the LSB plane of the cover image. When only LSB is changed, a slight change in intensity is there between original and reconstructed pixel, which is hard to detect visually. Hence, the presence of a message inside the image cannot be identified [5].

Example:

Cover Image:
10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011
Message Image: 101101101
Steganographed Image:
10010101 0000110**0** 11001001
1001011**1** 0000111**0** 1100101**1**
10011111 00010000 11001011

Thus, Cover Image + Concealed information = Stego Image
This formula gives a generic description of the steganographic process [5].

2. Related Work:

There have been lots of techniques to implement Steganography. According to the approach proposed in [6], LSB technique is applied using the theory of human visual cell sensitivity. It achieves high imperceptibility and robustness. According to the approach proposed in [7], LSB technique is applied and a secret key is applied to hide the information into a cover image. It provides better image quality and a better PSNR value. According to the approach proposed in [8], Least Significant Nibble is substituted with the secret data and AES encryption is also applied to the data.. It achieves high PSNR values. According to the approach proposed in [9], a comparative analysis is done between the different encrypting techniques like DES, AES and

RSA taking into consideration, the encryption ratio, scalability and other factors. It is concluded that AES algorithm gives good results as compared to DES and RSA.

2.1 Advanced Encryption Standard [6]

Advanced Encryption Standard(AES) is an encryption standard recommended by NIST. 128 bits data block is encrypted using AES and it uses key length of 128, 192 or 256 bits. We have used key length of 128 bits. The steps of AES algorithm are:

STEP 1. Derive the set of round keys from the cipher key.
STEP 2. Initialize the state array with the secret data.
STEP 3. Add the initial round key to the starting state array.
STEP 4. Perform nine rounds of state manipulation.
STEP 5. Perform the tenth and final round of state manipulation.
STEP 6. Copy the final state array out as the encrypted data.

2.2 AES Encryption Round [7]

Encryption process requires four types of operations.

STEP 1.Substitute bytes : Every byte is converted into a different value in this substitution operation.
STEP 2. ShiftRows : Rotation is performed on each row to the right by a certain number of bytes.
STEP 3. MixColumns : A new column is produced by separately processing each column of the state array. The old column is replaced by the new column.
STEP 4. XorRoundKey : The existing state array is taken and a XOR operation is applied with a portion of key.

2.3 AES Decryption Round [8]

Decryption requires inverse functions like InvSubBytes, InvShiftRows, InvMixColumns[9][10].

3. Proposed Technique:

The proposed technique has a two step implementation:

1.The secret message is transformed to cipher text by AES cryptography.
2.The cipher text is hidden inside the image using the modified LSB method.

3.1 Modified LSB Method

1. Until the cipher text length, convert each character of the cipher text to binary format according to the ASCII code and embed the cipher text being created from AES Encryption in the LSB's of cover image in the following order :

B1,B2,……..,Bn
G1,G2,……..,Gn R1,R2,……..,Rn
where B,G and R represent the blue, green and red components of a pixel.

2. The substitution is done on the LSB's of the cover image with the cipher text.

3. After the insertion is done in the LSB's, then find the 2nd and 3rd LSB's of the blue pixel.

4. Consider 2 bit combinations of (00,01,10,11) in the 2nd and 3rd LSB's of blue pixel and count the number of blue pixels with the highest pattern.

5. Invert the LSB's of the blue pixels with the highest pattern.

3.2 Implementation

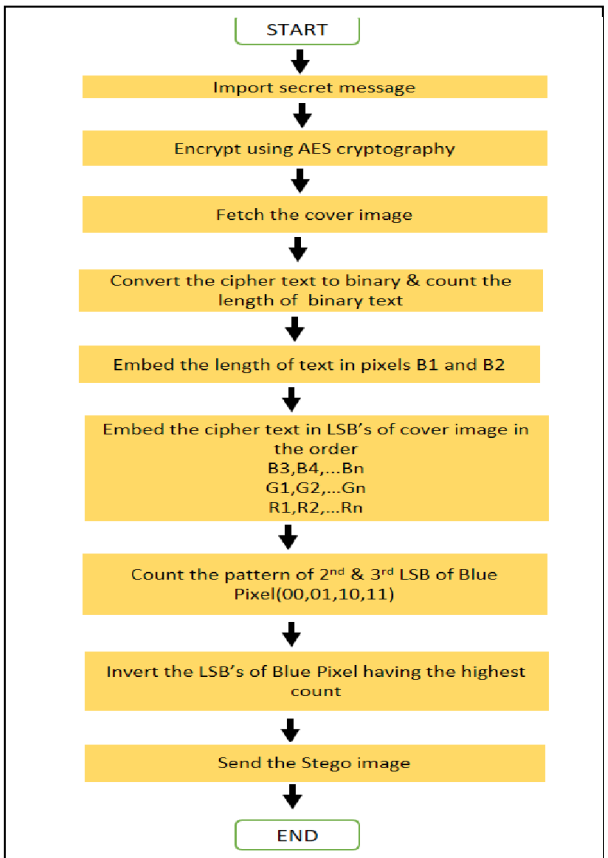


Fig.3. Hiding the secret message.

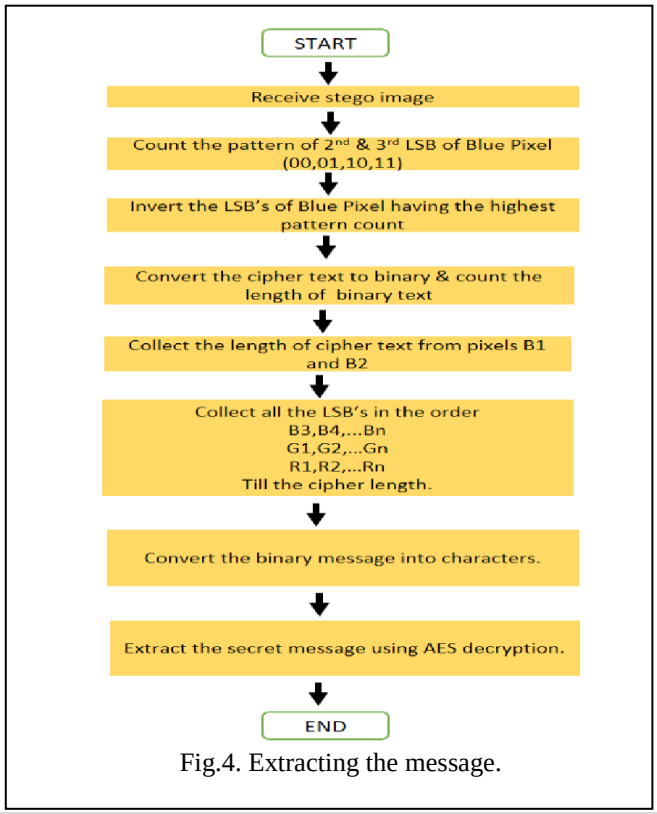
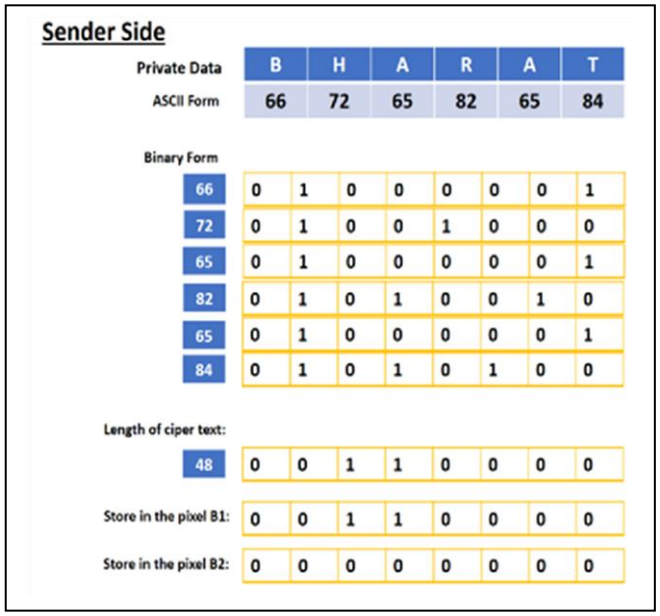
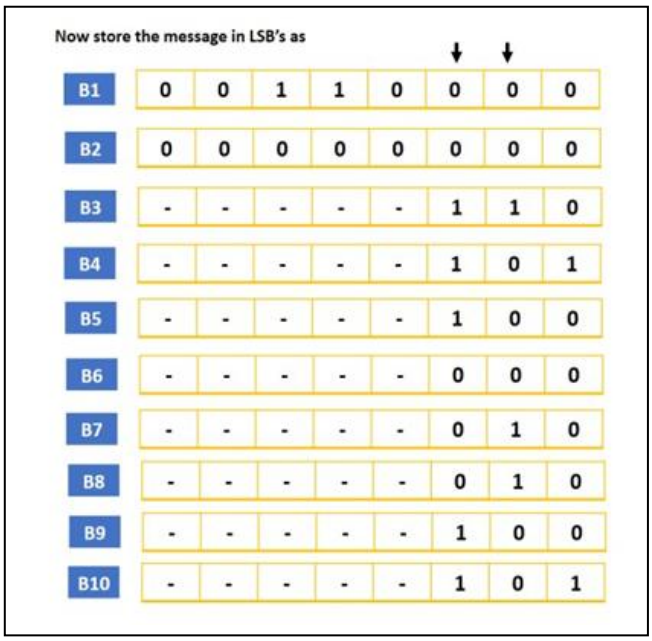


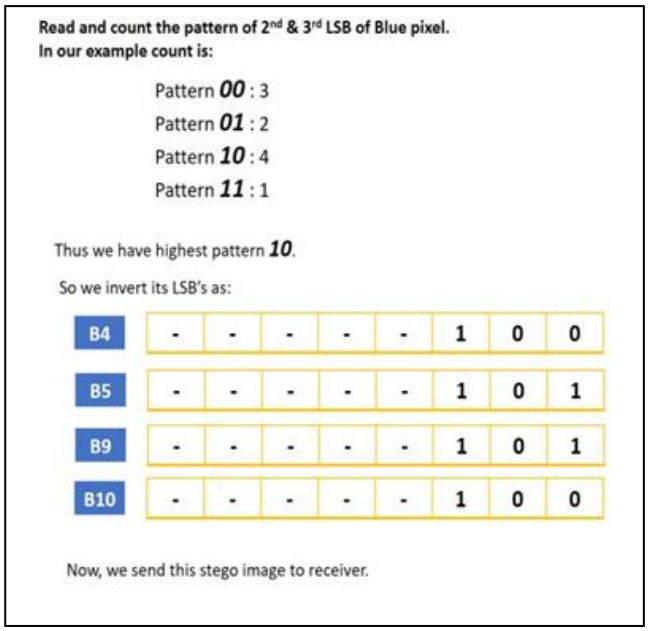
Fig.4. Extracting the message.

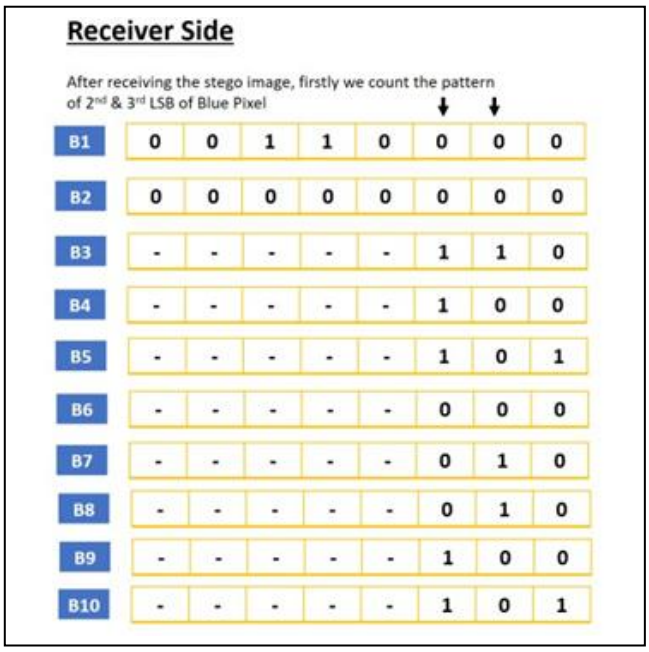
Example

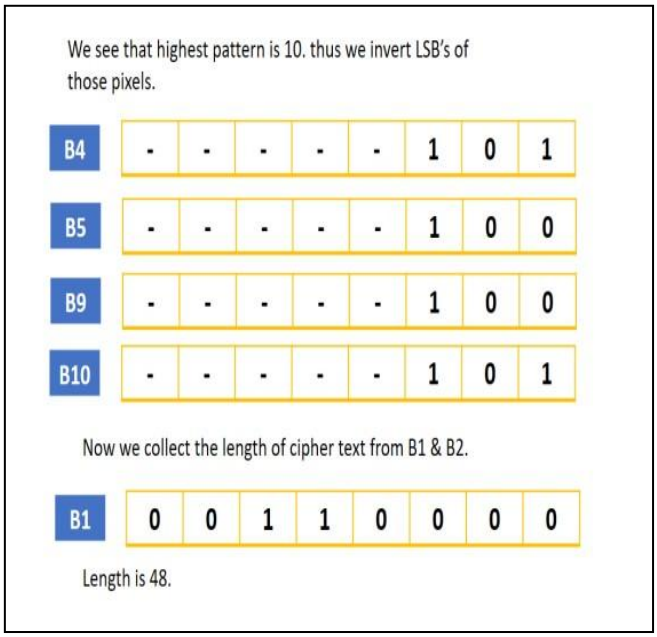
We are implementing the methodology, by the following example,

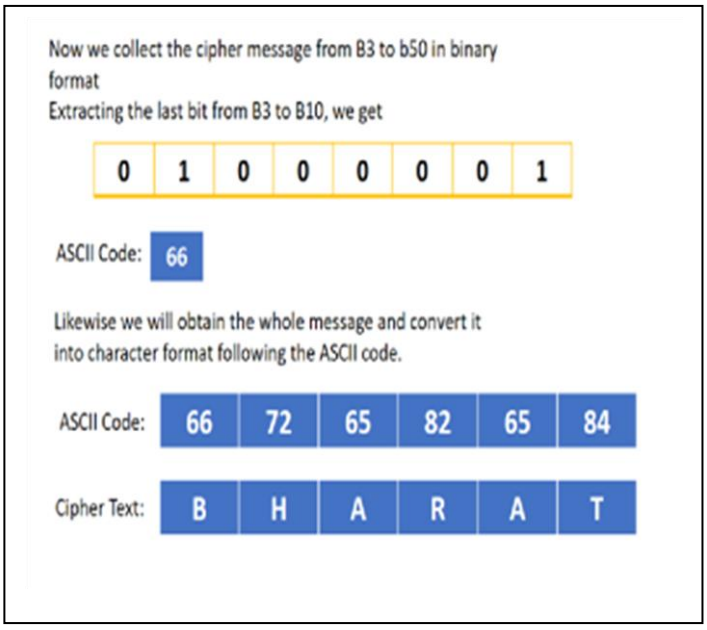





Read and count the pattern of 2nd & 3rd LSB of Blue pixel.
In our example count is:
Pattern 00 : 3
Pattern 01 : 2
Pattern 10 : 4
Pattern 11 : 1
Thus we have highest pattern 10.
So we invert its LSB's as:
B4 - - - - - 1 0 0
B5 - - - - - 1 0 1
B9 - - - - - 1 0 1
B10 - - - - - 1 0 0
Now, we send this stego image to receiver.


Receiver Side
After receiving the stego image, firstly we count the pattern of 2nd & 3rd LSB of Blue Pixel
B1 0 0 1 1 0 0 0 0
B2 0 0 0 0 0 0 0 0
B3 - - - - - 1 1 0
B4 - - - - - 1 0 0
B5 - - - - - 1 0 1
B6 - - - - - 0 0 0
B7 - - - - - 0 1 0
B8 - - - - - 0 1 0
B9 - - - - - 1 0 0
B10 - - - - - 1 0 1





4. Experimental Setup

The proposed method ensures double layer security with AES Cryptography and modified LSB where embedding of secret message starts with the least significant bit of the blue component of the pixel and human eyes are least sensitive to the difference in blue colour. The approach is analysed using characteristics MSE and PSNR. The following images are taken from USC-SIPI image database which are used in research in theoretical foundation and image processing.

Name	Cover Image	Stego Image
Airplane		
Couple		
House		
San Diego		

Table 1. Result of Modified LSB steganography

5. Comparative Study

Image enhancement or improving the visual quality of a digital image varies from individual to individual and is very subjective. In order to compare the effects of image steganography algorithms on image quality, essential quantitative/empirical measures are adopted. Here we use two error metrics to compare the quality of cover image and the stego image. The MSE represents the cumulative squared error between the previous image and the new image thus formed, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the less is the error, and best are the results.

MSE- Mean Square Error- It is the average of the squares of the errors or deviations that is, the difference between the estimator and what is estimated.

PSNR- Peak Signal to Noise Ratio- PSNR is calculated in decibels (dB). 40 dB and above should be the value of a high quality stego image. PSNR value is defined by the mean square error (M.S.E) for two images, It is the ratio between the maximum possible pixel value MAX of the image and the mean square error where x as well as y are image coordinates, SGxy (stego image) and CVxy(cover image) .
PSNR = 10 log10 ($^{MA}MSE^{X}$), where MAX is the maximum fluctuation in the original image.

TABLE 2. COMPARATIVE ANALYSIS OF MSE AND PSNR METRICS

IMAGE (BMP)	MEAN SQUARE ERROR		PEAK SIGNAL TO NOISE RATIO	
	CLASSICAL LSB	MODIFIED LSB	CLASSICAL LSB	MODIFIED LSB
AIRPLANE	0.00042	0.00036	79.37	82.49
COUPLE	0.00148	0.00137	74.12	76.75
HOUSE	0.00154	0.00149	70.23	76.38
SAN DIEGO	0.00046	0.00037	76.56	82.35

6. Conclusion

The proposed method is a good way to embed the hidden information without the risk of compromising its security. The secret information is concealed inside an image using a technique known as Image Steganography. For additional benefits, the content of the secret message is scrambled using Cryptography to avoid intrusion to unauthorised users and ensure safety during unfavourable situations. When the secret information is stored inside the original image, the new image thus formed is the stego image. AES Cryptography provides good results, as it ensures that even though the existence of message is detected, it is not easy to determine its contents. Modified LSB technique also proves to be very helpful in preserving the security of the information inside the image. There are almost negligible chances for the unauthorized users to recognise significant and noticeable changes in the stego image. The amplitude of change in both the images is not human perceptible. The use of both the techniques gives a way to secure the information from illegal users.

7. References

[1]. S. Katzenbeisser, & F.A Petitcolas, "Information Hiding techniques for steganography and digital watermarking", Boston, Artech House, 2000, pp.17-18.

[2]. A.Cheddad, J.Condell, K.Curran & P.Mc Kevitt, "Digital Image Steganography :Survey and Analyses of Current Methods",Signal Processing, Volume 90, Issue 3, March 2010, pp. 727-752.

[3]. Neil F. Johnson, & Sushil Jajodia, "Exploring Steganography:Seeing the Unseen", Computing Practices, February 1998., pp.26-34.

[4]. Arihant Khicha, & Neeti Kapoor, "Information System Security", Jaipur, Genius Publications, 2013, pp.2.33-3.34.

[5]. Nadeem Akhtar, Shahbaaz Khan, & Pragati Johri, "An Improved Inverted LSB Image Steganography", International Conference on Issues and Challenges in Intelligent Computing Techniques(ICICT 2014), pp. 749-750.

[6]. Vijay Anand J, & Dharaneetharan G D, "New Approach in Steganography by Integrating Different LSB Algorithms and Applying Randomization Concept to Enhance Security", Proceedings of the International Conference on Communication, Computing & Security , 2011, pp.474-476.

[7]. S.M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011) 22-24 December, 2011, Dhaka, Bangladesh.

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

[9]. B.Padmavathi, & S.Ranjitha Kumari, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique ", International Journal of Science and Research (IJSR), India, Volume 2 Issue 4, April 2013, pp.170-174.

[10]. Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal & Md. Delowar Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", 3rd International Conference on Informatics, Electronics & Vision 2014.

[11]. The USC-SIPI Image Database.