Enhanced LSB Approach With Huff-HIS Modeling For Secured Image Steganography

Harpreet Kaur
M.Tech. Student
CSE Dept.
Ramgarhia Institute of Engineering
and Technology
Punjab, India.
1182bains@gmail.com

Varinderjit Kaur
M.Tech. HoD
CSE Dept.
Ramgarhia Institute of Engineering
and Technology
Punjab, India.
Vari006rupi@gmail.com

Dr. Naveen Dhillon
Principal
Ramgarhia Institute of Engineering
and Technology
Punjab, India.
principal@riet.ac.in

***Abstract*— the security of the shared data is the major concern nowadays. Thus various data security mechanisms such as cryptography, encryption, data hiding etc has been developed till now. Steganography is the one of the prominent methods for securing the data. In this a cover file is used to hide the confidential data behind it. The steganography can be of various types like text steganography, image steganography, video steganography, audio steganography etc. In this work, an image steganography technique has been developed in order to enhance the security of the hidden text. For this purpose, the Huffman encoding and LSB mechanism is utilized. As the Huffman encoding is used to compress the text and LSB is used to hide the data behind the image file. The implementation of the proposed work is done in MATLAB. Along with this to prove the efficiency of the proposed work, a comparison analysis has been developed among 1-LSB, 2-LSB, LF-DCT, MF-DCT and proposed work. On the basis of the observations, the MSE, PSNR and Entropy of the proposed work is found to be effective than traditional mechanisms.**

Keywords*— image security, image steganography, Huffman Encoding, Least significant bit

I. INTRODUCTION

Consequently, Steganography is the procedure to hide the information before transmitting it to the receiver. Information can be covered up inside another digital medium, such as text, image, audio or video [1]. With the application of this technique intruder will not be able to suspect the existence of the message. Steganography can be associated with cryptography. The basic concept or inspiration behind execution of image Steganography is to communicate between the individuals with no fear of being assaulted of messages [2]. It has been utilized in a few regions including military, intelligence operatives, or bureaus because of its merits. These fields of espionage requisite a mechanism that can hide their crucial information and no intermediate person can calculate the meaning of the information [3]. The major concern of utilizing Steganography is to evade the concentration of the attacker from the hidden data in the transmission as if attacker would realize that there is hidden information in the transmitted message then observer will attempt every feasible concept so that he can read the hidden information [4].Following depicts the model of Steganographic procedure with cryptography:

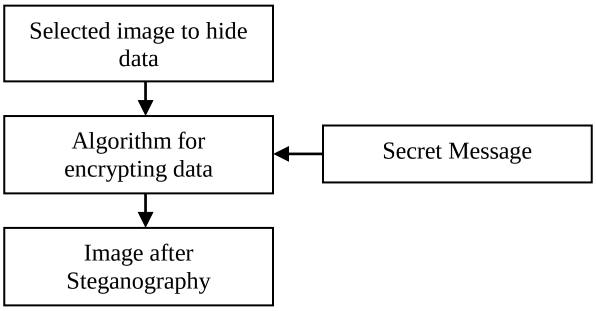
Selected image to hide data
Algorithm for encrypting data
Secret Message
Image after Steganography

Figure 1 building block of Steganography

In this study, a novel approach has been developed to enhance the security of the data that is hidden behind the image file. For establishing the objective, the proposed work uses the Huffman Encoding mechanism and Least Square Bit (LSB). The Huffman encoding is used to compress the text so that it could be secured from attackers or unauthorized users. The Huffman encoding is preferred because it is considered as the best encoding mechanism due to its feature of lossless compression.

II. PROBLEM FORMULATION

Security of the data is one of the major concerns. Various Steganography techniques have been proposed earlier but still the required results were not achieved. On the basis of literature review it is founded that the technique that was widely used for the purpose of image Steganography was DCT (Discrete Cosine Transformation). The major drawback of using DCT as embedding mechanism is that when inverse of DCT is applied for extracting purpose it leaves a block effect on the image. Block effect refers to the scenario when that area of the image is highlighted in which the data is embedded. Thus it makes easy for the intruders to find the location the embedded data. Another issue of the traditional DCT based image steganography is that it uses simple key to encrypt the data and it becomes a security threat if the intruders gains the access to the key.

III. PROPOSED WORK

In order to resolve the security and data embedding related issues in traditional DCT based image steganography mechanism, the proposed work implements the LSB data hiding technique along with the Huffman encoding mechanism. In proposed work, initially the image is extracted from the input dataset and then the image is converted to the HSI color model. The reason behind implementing the HSI is to extract the area from the image with high intensity. After extracting the area, the Huffman encoding is applied to the input data in order to compress it. After compressing the LSB (Least Significant Bit) technique is used as an embedding mechanism for hiding the data. Moreover, it can achieve a relatively high embedding capacity with no visual distortion in the resultant stego image. This work will also demonstrate the competitive performance of the proposed system in comparison with other systems. The workflow of proposed work is divided in two processes i.e. Embedding Process and Embedding Process. This section describes the methodology of both processes.

a) Embedding Process

Step 1. The foremost step for steganography in proposed work is to select the input image as a cover fie. The selection of input image is done from the available dataset of images.

Step 2. After selecting the image as input image, next step is to convert the format of the image. As the selected image is in RGB format, therefore it is firstly converted to the HSI format by using HSI model. For this purpose the formulation is as follows:

$$r = \frac{R}{R+G+B}, g = \frac{G}{R+G+B}, b = \frac{B}{R+G+B} \dots\dots (1.1)$$

Following normalized HIS component is observed:

$$h = \left\{\frac{0.5[(r-g)+(r-b)]}{[(r-g)^2+(r-g)(g-b)]^{1/2}}\right\} h \in [0,\pi] for\ b \leq g \dots (1.2)$$

$$h = 2\pi - cos^{-1}\left\{\frac{0.5[(r-g)+(r-b)]}{[(r-g)^2+(r-g)(g-b)]^{1/2}}\right\} h \in [0,2\pi] for\ b > g \dots (1.3)$$

$$s = 1 - 3.min(r,g,b); s \in [0,1] \dots . (1.4)$$

$$i = \frac{R+G+B}{3.255} \quad i \in [0,1] \dots\dots . (1.5)$$

Step 3. After converting the format of the image to HSI, the LSB is applied to the Intensity from Hue and Saturations.

Step 4. In this step, the input text is entered by the user. This text is going to embed behind the selected cover image.

Step 5. Then the Huffman encoding is applied to the entered text. The Huffman encoding is a mechanism that is applied to compress the text that has entered. It is preferred because it is lossless data compression mechanism.

Step 6. After applying the Huffman encoding to the text, the data is embedded behind the selected cover image by using LSB mechanism of data hiding.

The diagram in figure 2 represents the flow of the proposed work for embedding process.

b) Extracting Process

Step 1. For this first step is to select the stego image.

Step 2. Then the format of the stego image is converted to the HSI from RGB.

Step 3. After converting the image format, the information regarding the embedded data is extracted. Here information regarding the data hiding strategy is extracted such as the location of the pixel where the data is embedded.

Step 4. For extracting the data from the image, the information is used that is extracted in previous step. The extracted data is in the form of Huffman encoding, thus it is mandatory to decode the encoded data by applying Huffman decoding scheme. Hence the data is recovered from the stego image.

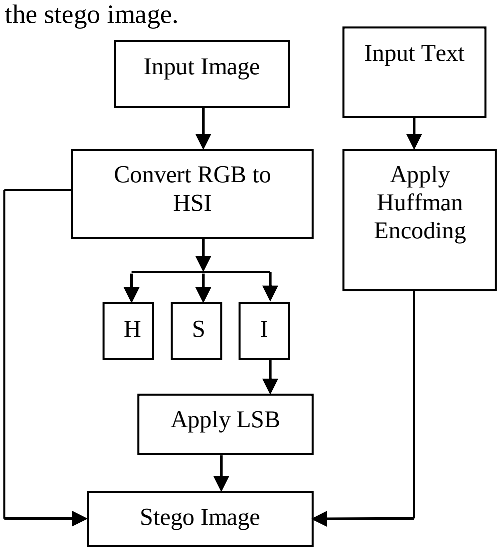

Figure 2 Data embedding Process of proposed steganography mechanism

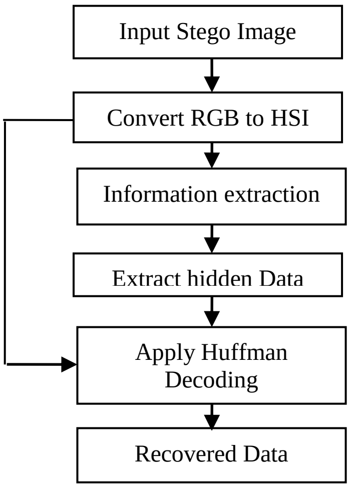

Figure 3 Data extracting Process of proposed steganography mechanism

IV. RESULTS ANALYSIS

In this work, a novel steganography mechanism has been developed by using the Huffman encoding and LSB data hiding scheme. The objective of the work is to design a secured image steganography technique. The proposed mechanism is implemented in MATLAB platform and is analyzed by using various input images. This section provides a review to the outcomes that are observed after implementation and analysis. The set of input images that are used in proposed work as cover image are as follows.

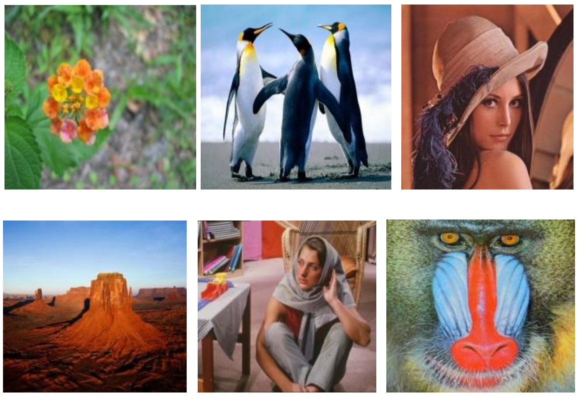

Figure 4 Set of Input images used for proposed work

While implementing the proposed image steganography technique, the analysis has been done by using various input images i.e. Mandrill, Lena and Flower. The performance analysis is done by using the following parameters:

a) Peak Signal to Noise Ratio (PSNR): PSNR is a parameter used to evaluate the noise in the image or signal with respect to signal. It defines as a ratio between the maximum signal and the noise. Signal in the process is considered as an original data and noise is the error in the data. PSNR can be expressed as an equation in db:

$$\text{PSNR} = 10.\,log_{10}\left(\frac{MAX_1^2}{MSE}\right) \dots\dots\dots\dots.1.1$$

$$= 20.log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right) \dots\dots\dots\dots\dots\dots\dots\dots.1.2$$

$$= 20.log_{10}(MAX_1) - 10.\,log_{10}(MSE)\dots.(1.3)$$

b) Mean Square Error (MSE): MSE is a parameter that defines the average error of an image. It is a difference between the estimator and the estimated value. It has used to estimate the quality of the proposed technique with respect to the traditional technique. Its value always is non-negative and closer to zero value is better.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \dots\dots\dots(1.4)$$

c) Entropy: There is variety of entropy evaluation techniques but the Shannon entropy is considered as the prominent once. The Shannon Entropy is a classical method and act as a base for other entropy methods as well. The basic formulation of Shannon entropy mechanism is as follows:

$$SE = -\sum\nolimits_{i=0}^{n} p_i log_2\, p_i \dots\dots.(1.5)$$

The graph in figure 5 elaborates the comparison analysis of proposed work and traditional work (1-LSB, 2-LSB, LF-DCT and MF-DCT) for the image of Mandrill. The comparative analysis is generated in the terms of PSNR. The x axis in the graph shows the message size as the minimum size of message in proposed work is 0 and the maximum size is considered to 1000. The range of PSNR is from 35dB to 60 dB. The observations from the given graph prove that the proposed work outperforms the traditional schemes. Similarly, the graph in figure 6 shows the comparison of proposed and traditional work for same image in the terms of MSE. The observed MSE of proposed work is found to be lower than the MSE of traditional work.

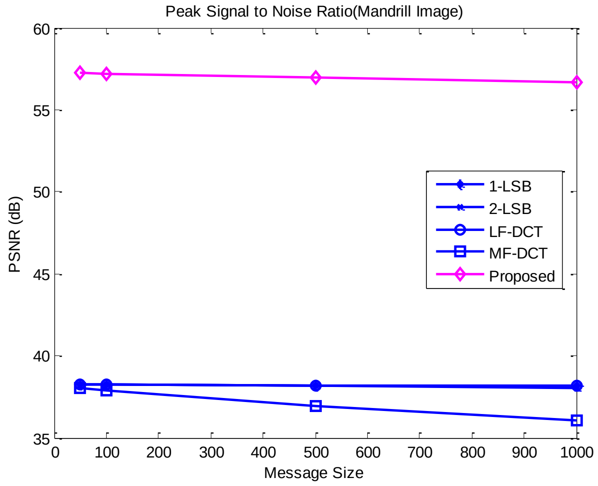

Figure 5 PSNR evaluations of Proposed Work and Traditional Work (Mandrill Image)

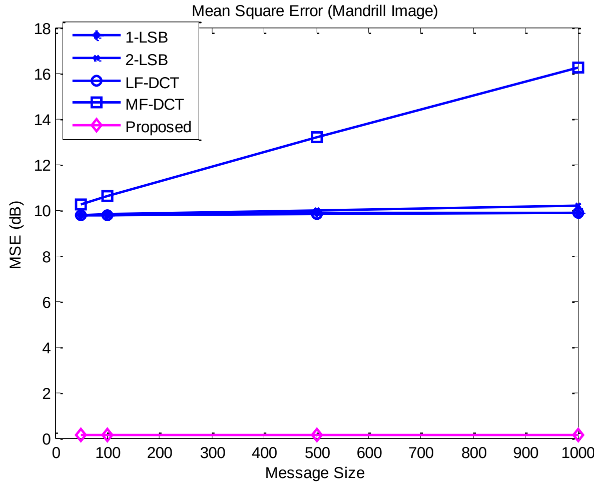

Figure 6 MSE evaluations of Proposed Work and Traditional Work (Mandrill Image)

The PSNR of proposed work for the image of Lena is shown in graph of figure 6. The graph delineates the performance of proposed and traditional work with respect to the PSNR. The graph manifests that the PSNR of the proposed work is higher in comparison to the traditional works. Similarly, the graph in figure 8 represents the MSE analysis of proposed work, 1-LSB, 2-LSB, LF-DCT and MF-DCT. The graphical facts delineates that the MSE of proposed work outperforms the MSE of traditional mechanisms.

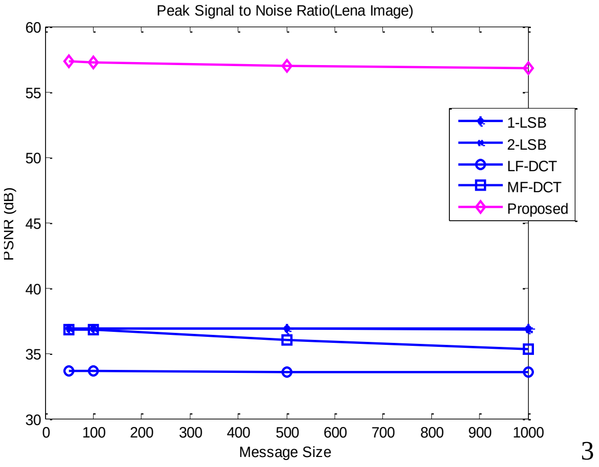

Figure 7 PSNR evaluations of Proposed Work and Traditional Work (Lena Image)

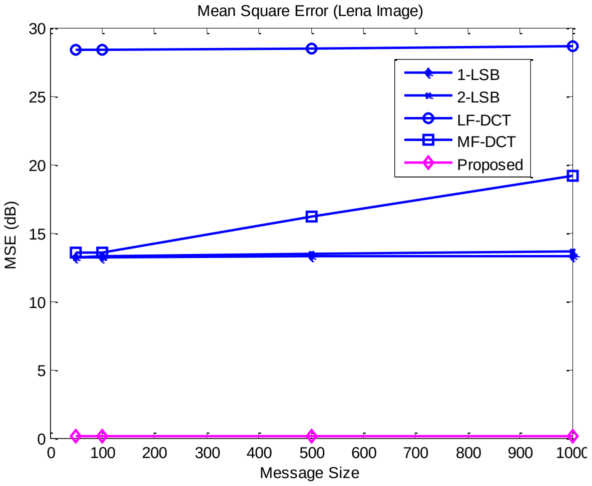

Figure 8 MSE evaluations of Proposed Work and Traditional Work (Lena Image)

The graph in figure 9 explains the PSNR of proposed work and traditional work for the image of flower.

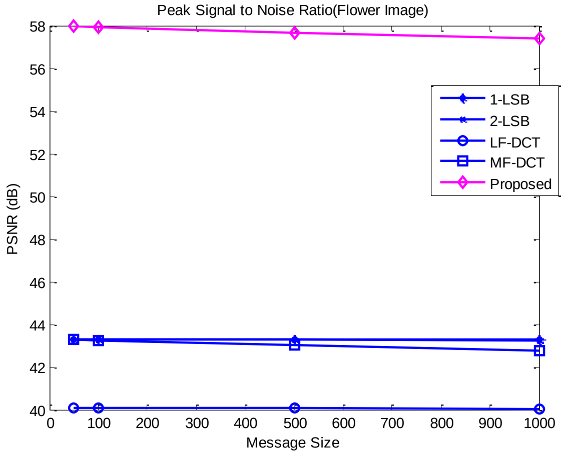

Figure 9 PSNR evaluations of Proposed Work and Traditional Work (Flower Image)

The Peak Signal Noise Ratio defines the ratio of information to the noise in the signal. Therefore, it is mandatory to have higher PSNR value. The signal with lower PSNR value defines that the signal is having high noise in comparison to the informative signals. The PSNR of proposed work is higher for the image of flower

The Mean Square Error refers to the errors found in output signals. The MSE of ideal system or signal should be low. The graph in figure 10 defines the comparison analysis of proposed and traditional work for the image of flower. The MSE of proposed work in this case is 0 whereas the MSE of traditional techniques is higher than 3 and 6 respectively. Therefore, it is proved that the proposed work is more efficient than the traditional work.

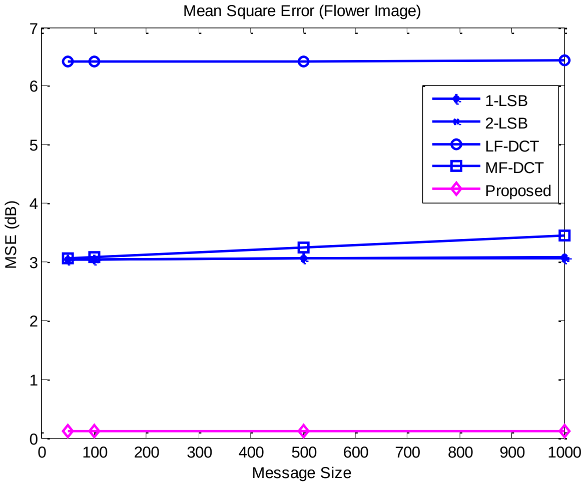

Figure 10 MSE evaluations of Proposed Work and Traditional Work (Flower Image)

The entropy evaluation for cover and final stego image in case of proposed work is shown in figure 11. The entropy evaluation is done for three of the images as shown in graph i.e. Mandrill, Lena and Flower.

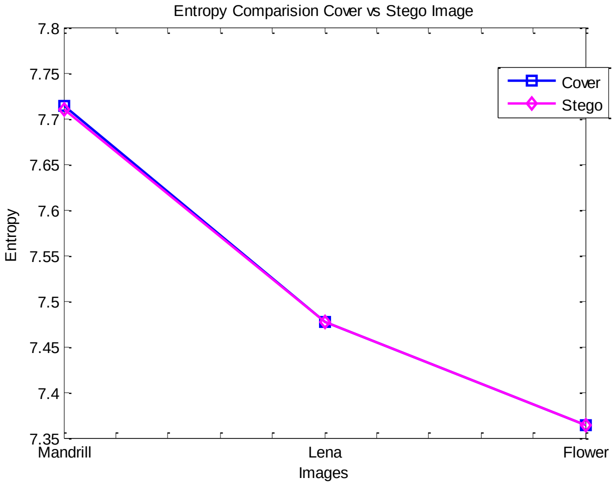

Figure 11 Entropy evaluations of Proposed Work

The y axis in the graph calibrates the values for entropy and it ranges between 7.35 and 7.8. The graph shows that the entropy for the image of mandrill is 7.71 approximately, for the image of Lena it is 7.451 approximately and for the image of flower it is lower than 7.4 for both cover and stego images.

Thus, it is observed that the after embedding the text to the image file by using the proposed work, the entropy of the image has not changed.

V. CONCLUSION

On the basis of the observations from graphical results, it is concluded that the proposed work is quite effective and better than the traditional 1-LSB, 2-LSB, LF-DCT and MF-DCT mechanism in the terms of PSNR, MSE and Entropy. The analysis of the mechanism has been done on the basis of various input images such as image of mandrill, Lena and flower. The facts and figures obtained from the results proves that the PSNR of proposed work is higher than the PSNR of traditional works, MSE of proposed work is lower with respect to the traditional techniques. Consequently, the entropy evaluation defines that the proposed work did not leads to the variations in the cover image and stego image.

The proposed work could be enhanced in future in terms of data hiding capacity of the image. The technique with high data hiding capacity can hide the large text. Therefore, more amendments in proposed work can be done in near future.

REFERENCES

[1] Sahar A. El Rahman, “A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information”, Elsevier, 2016.

[2] Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on , vol., no., pp.97,100, 2013.

[3] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 2013.

[4] Lin Zhang, Jianhua Wu, Nanrun Zhou, “Image Encryption with Discrete Fractional Cosine Transform and Chaos”, Fifth International Conference on Information Assurance and Security 2009 IAS '09, pp 61 – 64, 2009.

[5] Parmar Ajit Kumar Maganbhai1, Prof. Krishna Chouhan2, “A Study and literature Review on Image Steganography”, IJCSIT, 2015.

[6] K. Thangadurai ; G. Sudha Devi, “An analysis of LSB based image steganography techniques”, IEEE, 2014.

[7] Sahib Khan ; Nasir Ahmad ; Muhmmad Ismail ; Nasru Minallah ; Tawab Khan, “A secure true edge based 4 least significant bits steganography”, IEEE, 2015.

[8] Bassam Jamil Mohd ; Saed Abed ; Thaier Al-Hayajneh ; Sahel Alouneh, “FPGA hardware of the LSB steganography method”, IEEE, 2012.

[9] Gotfried C. Prasetyadi ; Achmad Benny Mutiara ; Rina Refianti, “File encryption and hiding application based on advanced encryption standard (AES) and append insertion steganography method”, IEEE, 2017.

[10] Fatema Akhter, “A secured word by word Graph Steganography using Huffman encoding”, IEEE, 2016.

[11] G. Prashanti, K. Sandhyarani, “A New Approach for Data Hiding with LSB Steganography”, Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer, pp. 423-430, 2015.

[12] S. Goel, S. Gupta, N. Kaushik, “Image Steganography – Least Significant Bit with Multiple Progressions”, Springer, pp. 105-112, 2014.

[13] D. Baby, J. Thomas, G. Augustine, E. George, N.R. Michael, “ A Novel DWT based Image Securing method using Steganography”, International Conference on Information and Communication Technologies (ICICT), pp. 612-618, 2015.

[14] B. Feng, W. Lu, and W. Sun, “Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture”, IEEE transactions on Information Forensics and Security, Feb. 2015.

[15] M. Nusrati, A. Hanani and R. Karimi, “Steganography in Image Segments Using Genetic Algorithm”,IEEE, pp. 102-107, 2015.

[16] N. A. Al-Otaibi, and A. A. Gutub, “2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers”, Lecture Notes on Information Theory, June 2014, pp. 151-157.

[17] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, “An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography”, IEEE, pp. 1-6, 2014.

[18] K. Qazanfari and R. Safabakhsh, “A new Steganography Method which Preserves Histogram: Generalization of LSB++”, Elsevier, pp. 90-101, 2014.

[19] A. Nag, J.P. Singh, S. Biswas, D. Sarkar, and P.P. Sarkar, “A Huffman Code Based Image Steganography Technique”, 1st International Conference on Applied Algorithm (ICAA) , pp. 257-265, 2014.

[20] N. Akhtar, S. Khan and P. Johri, “An Improved Inverted LSB Image Steganography”, IEEE, pp. 749-755, 2014.