International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Text Embedded System using LSB Method

Win Win Maw[1], San San Lwin[2]

[1]Lecturer, Faculty of Computer System and Technologies, University of Computer Studies, Mandalay, Myanmar
[2]Lecturer, Department of Information System, Technological University, Kyaukse, Myanmar

How to cite this paper: Win Win Maw | San San Lwin "Text Embedded System using LSB Method" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.1818-1822, **https://doi.org/10.31142/ijtsrd26696**

IJTSRD26696

ABSTRACT

An important topic in the exchange of confidential messages over the internet is the security of information conveyance. For instance, the producers and consumers of digital products are keen to know that their products are authentic and can be differentiated from those that are invalid. The science of encryption is the art of embedding data in audio files, images, videos or content in a way that would meet the above security needs. Steganography is a branch of data-hiding science which aims to reach a describe level of security in the exchange of private military and commercial data which is not clear. This system is proposed to hide the text information files within the image based on the LSB method in order to meet security requirement such as confidential and integrity. The least significant bit is the bit which is farthest to the right and holds the least value in a multi-bit binary number. This system is implemented by using C# programming.

KEYWORDS: *C#, hiding text inside an image, Steganography, LSB, embedded*

1. INTRODUCTION

Data hiding is of importance in many applications. For hobbyists, secretive data transmission, for privacy of users etc. the basic methods are: Steganography and Cryptography. Steganography is a simple security method. Generally there are three different methods used for hiding information: steganography, cryptography, watermarking. In cryptography, the information to be hidden is encoded using certain techniques; this information is generally understood to be coded as the data appears nonsensical. Steganography is hiding information; this generally cannot be identified because the coded information doesn't appear to be abnormal i.e. its presence is undetectable by sight. Detection of steganography is called Steganalysis.

Steganography is of different types:

- ➢ Text steganography
- ➢ Image steganography
- ➢ Audio steganography
- ➢ Video steganography

In all of these methods, the basic principle of steganography is that a secret message is to be embedded in another cover object which may not be of any significance in such a way that the encrypted data would finally display only the cover data. So it cannot be detected easily to be containing hidden information unless proper decryption is used.

The security of information becomes one of the most important factors of information technology and communication because of the huge rise of the World Wide Web and the copyright laws. Information hiding can be achieved into four phases are: preliminary phase in which an encryption technique is applied. Embedded phase in concerned with algorithms which are used for information hiding. The transmission phase and finally the extraction phase. For each step a security issue must be considered. Information hiding can be used in different applications include copyright, military, confidential communication, digital elections, E-commerce, copy control, authentication. Hiding information is better than ciphering in the aforementioned fields, because in the former, nobody can notice any information hiding for a message in image. In steganography, image has become an essential, potential, and popular file to be used as the carrier file for protecting the confidential information. But actually, the theory had said that all of the digital files could be used as a carrier file or the message.

The secret message, cover message, embedding algorithm and the secret key are the main four terminologies used in the steganography systems. The secret message is defined as the data or information which is needed to be hidden in the appropriate digital media. While the cover message is considered as the carrier of the hidden message such as image, video, text or any other digital media. The embedding algorithm is the most important part; it can be defined as a method or the ideas that usually used to embed the secret information in the cover message to prevent unauthorized people to get it. The LSB coding is suitable to work with any type of data file format, hence easily combine with any technique, but unfortunately, LSB encoding lack robustness and security. In this technique the data are only hidden in the last bit, which lower its importance. In this technique, an attacker can easily identify and uncover the message by just removing the complete LSB plane. Many improvements have been taken to enhance the performance of LSB coding, for more details see:

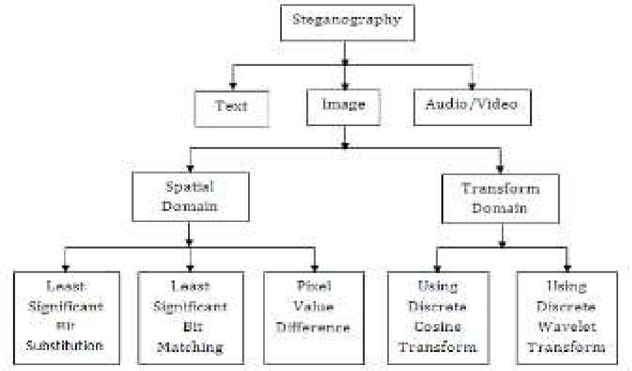

Steganography
Text
Image
Audio/Video
Spatial Domain
Transform Domain
Least Significant Bit Substitution
Least Significant Bit Matching
Pixel Value Difference
Using Discrete Cosine Transform
Using Discrete Wavelet Transform

Figure: 1.1 performance of LSB coding

As the above explanation goes, every steganography consists of three components:

- Cover object
- Message object
- Resulting Steganographic object

With the rapid development of internet and wide application of multimedia technology, people can communicate the digital multimedia information such as digital image, with others conveniently over the internet. In numerous cases, image data, transmitted over a network are expected not to be browsed or processed by illegal receivers. Consequently, the security of digital image has attracted much attention recently and many different methods for image encryption have been proposed, such as Optical systems are of growing interest for image encryption because of their distinct advantages of processing 2-dimensional complex data in parallel at high speed. In the past, many optical methods have been proposed in. Among them the most widely used and highly successful optical encryption scheme is double random phase encoding proposed in. It can be shown that if these random phases are statistically independent white noise then the encrypted image is also a stationary white noise. In some schemes , chaos based functions are used to generate random phase mask.

In this system LSB substitution method is implemented and DCT method is discussed for image steganography. Visual Studio C# 2010 is used for coding. The codes and result images are in the following report.

2. PROPOSED SYSTEM

In this paper, this system proposed a new steganographic algorithm that is used to hide text file inside an image. In order to increase/maximize the storage capacity used a compression algorithm that compresses the data to be embedded. The compression algorithm used works in a range of l bit to 8 bits per pixel ratio. By applying this algorithm developed an application that would help users to efficiently hide the data.

In this present digital scenario secure and invisible communication between two parties is the prime requirement. Steganography is the technique of hidden communication. It not only hides the message contents, instead it hides the existence of the messae. It hides the message in such a way that message will be imperceptible to the human eyes. Least Significant Bits(LSB)Technique is Spatial Domain Technique. It hides the secret message inside an image. In this technique the least significant bit of the cover image is used for concealing the bit value of secret message, for providing higher security in digital communication.

The mass diffusion of digital communication needs the special means of security. Cryptography concentrates on rendering the message unreadable to any unauthorized persons who might intercept them. In contrast, steganography is a method of concealing the existence of message to allow a secure communication in a complete undetectable manner. Digital image is the most common type of carrier used for steganography. In this paper, they have proposed a steganography, that reads the message and converts it to a colored image, that is transmitted to the authorized destination, and from which is extracted the information needed to reconstruct the original image. Encryption approach is based on analyzing the plain text and extracting from it its component's letters, which are encrypted in the colored image. This system show that for a message size in the range ($x_{1,}$ x_2) bytes, the size of the resultant image will be fixed and consequently the encryption and decryption time are fixed.

An important topic in the exchange of confidential messages over the internet is the security of information conveyance. For instance, the producers and consumers of digital products are keen to know that their products are authentic and can be differentiated from those that are invalid. The science of encryption is the art of embedding data in audio files, images, videos or content in a way that would meet the above security needs. Steganography is a branch of data-hiding science which aims to reach a desirable level of security in the exchange of private military and commercial data which is not clear. These approaches can be used as complementary methods of encryption in the exchange of private data.

In this present digital scenario secure and invisible communication between two parties is the prime requirement. Steganography is the technique of hidden communication. It not only hides the message contents, instead it hides the existence of the message. It hides the message in such a way that message will be imperceptible to the human eyes. Least Significant Bit(LSB) Technique is Spatial Domain Technique. It hides the secret message inside an image. In this technique the least significant bit of the cover image is used for concealing the bit value of secret message, for providing higher security in digital communication.

3. PROPOSED SYSTEM ARCHITECTURE

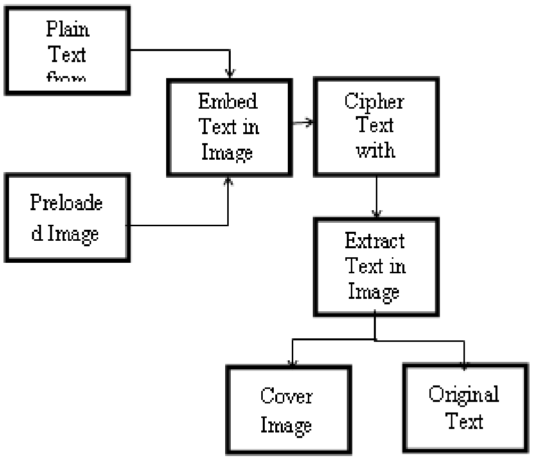


Figure 3.1 Block Diagram of Text Embedding in Image

4. WINDOW APPLICATION

The application has function and user interface that everyone is familiar.

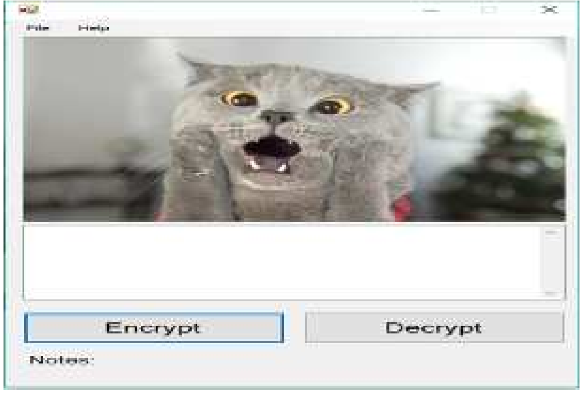


Figure 4.2 Main User Interface

In figure 4.3, after the image in the open menu item from file menu bar is clicked, the user can open the image.

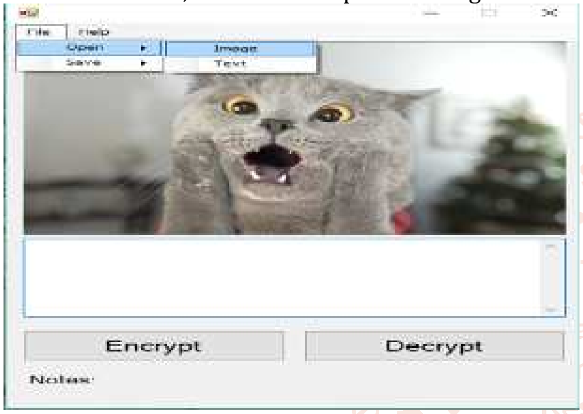


Figure 4.3 File Open Action

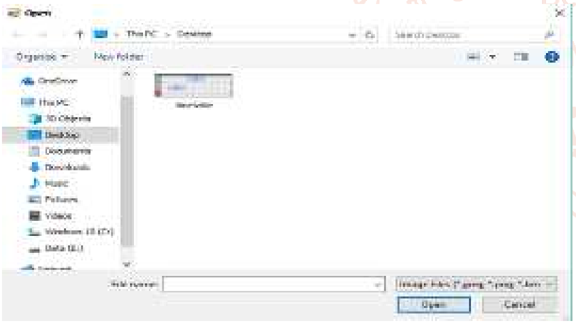


Figure 4.4 File Open Dialog Opened

In figure 4.5, the user also can get the text to input to the image from the text in the open menu item in the file menu bar.

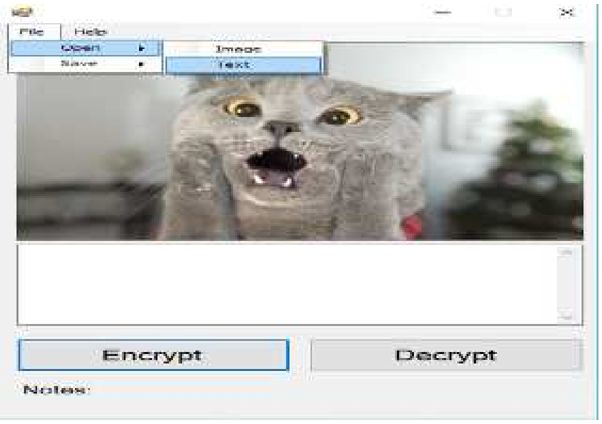
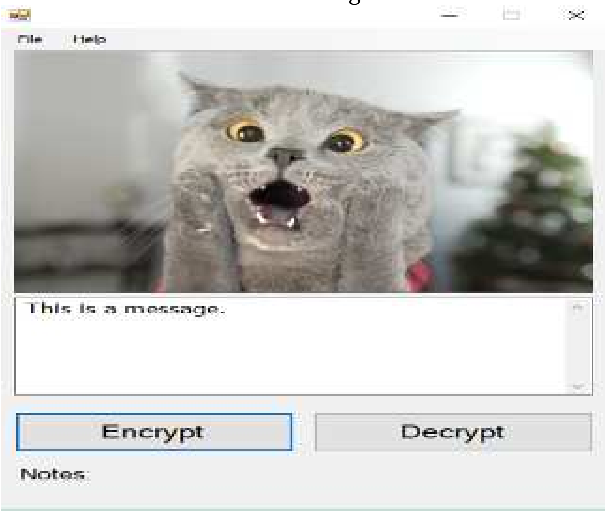


Figure 4.5 Text File Open Action

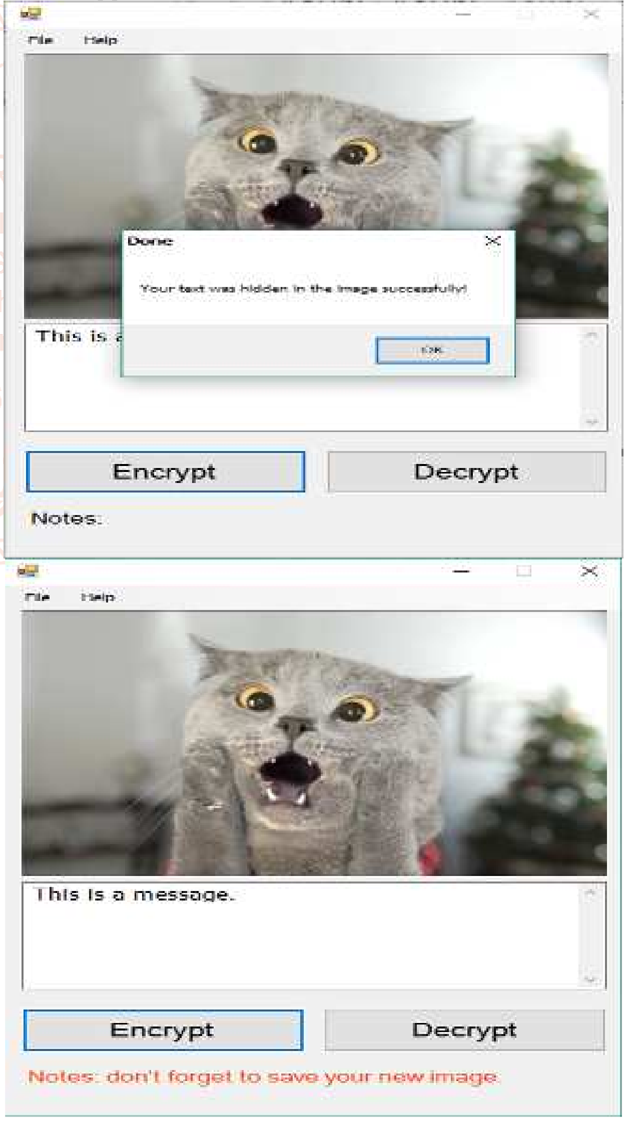
In figure 4.6, the user can click "Encrypt" button to embed the text in the text field to the image.



This is a message.

Figure 4.6 Opening File

In figure 4.7, after a text file has been opened, the text in the text file appears with the message box.



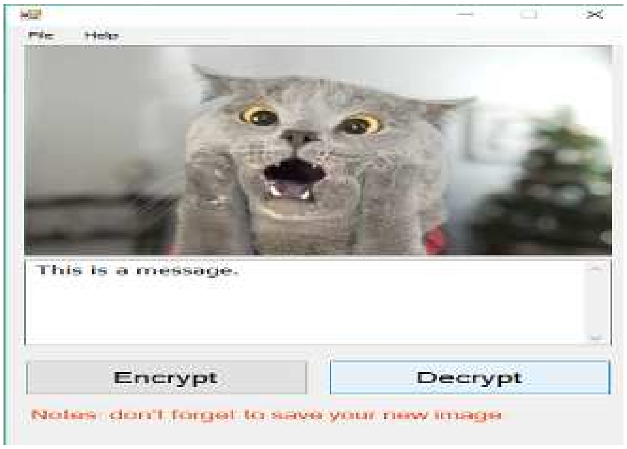
Your text was hidden in the image successfully!

This is a message.

Notes: don't forget to save your new image.

Figure 4.7 Sequence of Message after Embedding Text

After embedding text, the image in image box is not orginal file. It contains the text message.



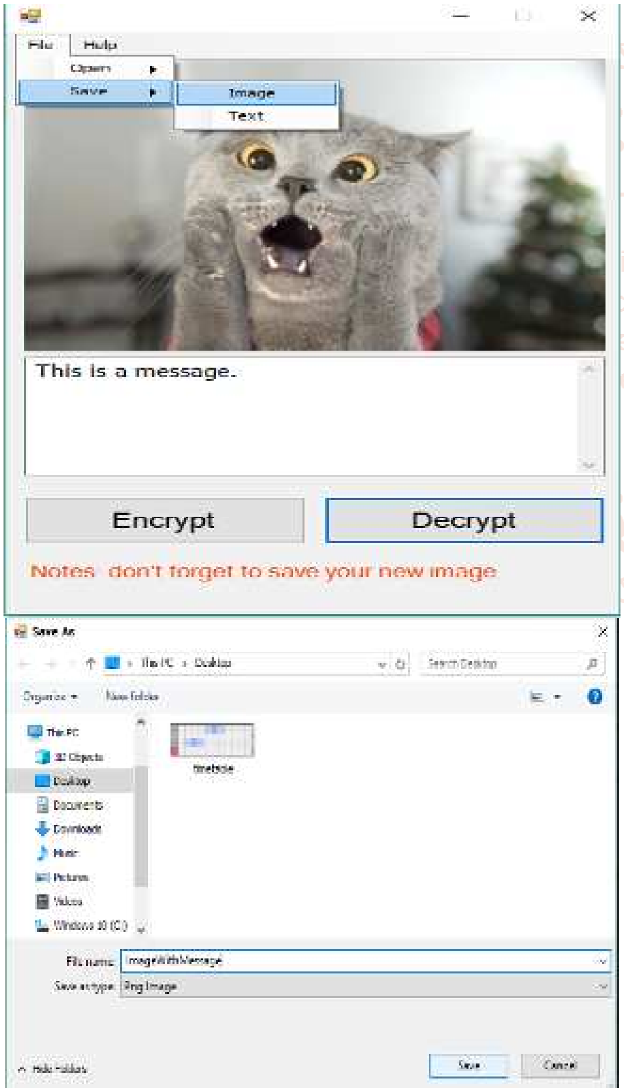
This is a message.

Notes: don't forget to save your new image

Figure 4.8. After Decrypt Button clicked

5. FILE SAVING

In figure 5.1 and figure 5.2, file saving action is also added for usefullness and flexibility of application. The user can save image from the image box or text from text box.



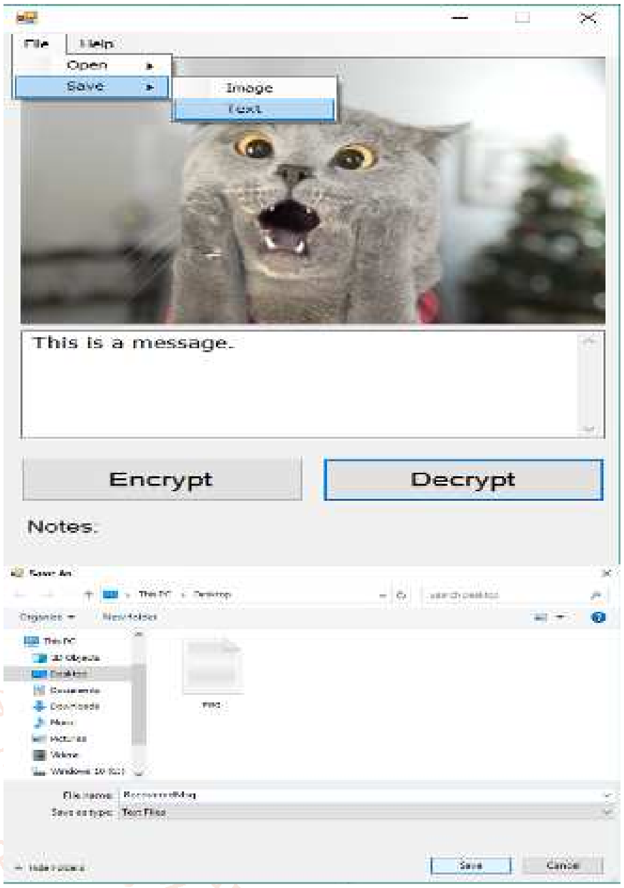
This is a message.

Notes: don't forget to save your new image

File name: ImageWithMessage

Save as type: Png Image

Figure 5.1. Image Save Action



This is a message.

Notes:

File name: RecoveredMsg

Save as type: Text Files

Figure 3.10. Text File Save Action

6. EXPERIMENTAL RESULTS

Experiments are demonstrative percentage and project evaluation.

6.1 Demonstrative Percentage

The users have run the application 20 times with different images to test whether the application run at any environment. The result is shown below.

With Many Different Images	
The application run smoothly?	90%

Table 6.1. The ability to run with different images

6.2 Project Evaluation

The application is send to 20 students and let them use this application for evaluation who are familiar with window applications. The feedback from them is as follows.

Application Features	Score (0 – 5)
Application has good UI	4.5
Application has good UX	4.6
Text Amount is enough for conversation	4.9
File Open and File Save Dialog are useful	4.8
Notifications and Notes are useful	4.5
The accuarcy of recovered text	5
Overall Satisfaction on the application	4.6
Total Scores	4.7

Table 4.2. The feedback for evaluation

7. CONCLUSION

An application is written to enable to embed text message in a picture for security reasons. The embedding is done starting from the top left pixel to bottom right pixel by going in normal hand writing direction. The text are converted into byte array and each bit of these bytes are embedded in the LSB of Red, Green and Blue bytes of pixel. After all the text are embedded, we add a byte of zero value to mark the end of text. The embedded image file can be saved in png format. That file can be opened and loaded again to the picture box. Then we can extract the message. In extraction process, the LSB of Red, Green and Blue bytes are read making eight bits into one byte which is one character. After seeing continuous zeros eight time, the reading is stopped. The recovered text will appear in the text box. These text can be saved in txt format.

7.1 Further Extension

There are many possibilities for improving this project. These are the two main features that are highly recommended in the future.

- In the software part, we might make the application as a chatting application that only communicate with images containing secret message and adding more security features like hashing the pixel of the images with a key.
- In text embedding part, we might make embedding randomly. Rather than embedding text in pixel in the normal direction, the sequence of pixel to embed is randomly used.

REFERENCES

[1] 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.

[2] 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), Procedia Computer Science, April 2015, pp. 612-618.

[3] 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 2015, pp. 423- 430.

[4] M. Nusrati, A. Hanani and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm", 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT), Feb 2015, pp. 102-107.

[5] Suma S. and Dharmambal. 2015. A Novel Image Steganography based on Secured Inversion Technique, International Journal of Innovative Research in Computer and Communication Engineering, 3(6).

[6] E. Dagar and S. Dagar, "LSB based Image Steganography using X-Box Mapping", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 2014, pp. 351-355.

[7] K. Qazanfari and R. Safabakhsh, "A new Steganography Method which Preserves Histogram: Generalization of LSB++", Elsevier International Journal of Information Sciences, Sept. 2014, pp. 90-101.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) , Jan. 2014, pp. 257-265.

[8] 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.

[9] N. Akhtar, S. Khan and P. Johri, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Feb. 2014, pp. 749-755.

[10] 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 International Conference on Informatics, Electronics & Vision (ICIEV), May 2014, pp. 1-6.