International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 12 | Dec -2016 www.irjet.net p-ISSN: 2395-0072

# IMAGE STEGANOGRAPHY USING LSB BIT-PLANE SUBSTITUTION

**(1) TANMAY SINHA ROY**

*(1) Dept. of ICE, Assistant Professor,Haldia Institute of Technology, Haldia- 721657, WB, India*
*Email-tanmoysinha.roy@rediffmail.com*

**ABSTRACT---**Image Steganography plays vital role in digital image processing. The purpose of image Steganography is to conceal a file, message, image or video within another file, message, image or video. The advantage of Steganography over Cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Thus, cryptography is the practice of protecting the contents of a message alone, whereas steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.Any digital image is comprised of pixels of different size of matrices, various Image Steganography algorithms have been developed. In this paper, we have used the BIT-PLANE substitution method to hide a Messase image into a Cover image. we have considered two uint8 digital images, one is the cover image and the other is the message image. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the message image to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object as few LSB bits of the cover object are replaced. In this paper, we have obtained different stego-images based on the number of LSB bits we have substituted in the cover image for the given message image. Also we have calculated the PSNR(Peak To Noise Ratio) and MSE(Mean Squared Error) of different Stego Images for different LSB bit substitutions. Here, we have replaced 1 to 4 LSB bits in the cover image without destroying the content in the cover image significantly to hide the message image into it. We have not gone further with replacing above 4 bits as the content of the cover image gets changed then.

**KEYWORDS-** Steganography, Cryptography, Stego-Image, PSNR, MSE

## 1. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images. Image processing is one of the most important area of multimedia applications and it is known, these applications can be found almost everywhere in the modern world. Because of that, the number of people working with images is rapidly increasing which means, that demand for image processing tools also grows. Images are being compressed, decompressed, sent over the internet, modified or distorted in various ways and all these things affect their quality. It is the key element for multimedia to be able to assess the quality changes, predict them and eventually correct them. An image defined in the "real world" is considered to be a function of two real variables, for example a(x, y) with a as the amplitude (e.g. brightness) of an image at real coordinate position (x, y).An image may be considered to contain sub images also called as regions-of-interest or regions. Image is a collection of objects. The amplitude of a given image will always be either real number or integer number. A quantization process converts a continuous range (say between 0 and 100%) into a discrete number of levels. A sampling process that converts an analog image a(x, y) in a 2D continuous space to a digital image a [m, n] in a 2D discrete space is called digitization. The 2D continuous image a(x, y) is divided into N rows and M columns. The intersection of a row and a column is called a pixel.

Steganography is a branch of information hiding. It allows the people to communicate secretly. As increasingly more material becomes available electronically, the influence of steganography on our lives will continue to grow. Many confidential information were leaked to a rival firm using steganographic tools that hid the information in music and picture files. The application of steganography is an important motivation for feature selection. A new steganographic algorithm for

8bit(grayscale) or 24bit (colour image) is presented in this article, based on Logical operation. Algorithm embedded Ascii code of text in to LSB of cover image.

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. The data can be hidden in basic formats like:
Audio, Video, Text and Images etc.

The various types of steganography include:

*a. Image Steganography:* The image steganography is the process in which we hide the data within an image so that there will not be any perceived visible change in the original image. The conventional image steganography algorithm is LSB embedding algorithm.

*b. Audio Steganography:* Steganography can be applied to audio files i.e., we can hide information in an audio file, it can be called Audio Steganography. The audio file should be undetectable.

*c. Video Steganography:* Steganography can be applied to video files also. If we hide information in a video file, it can be called Video Steganography. The video file should be undetectable by attacker.

*d. Text files Steganography:* Steganography can be applied to text files also. If we hide information in a textfile, it is called Text Steganography.

**Terminology of Steganography**

**Cover-Image:** An image in which the secret information is going to be hidden. The term "cover" is used to describe the original, innocent message, data, audio, still, video etc. The cover image is sometimes called as the "host".

**Stego-Image:** The medium in which the information is hidden. The "stego" data is the data containing both the cover image and the "embedded" information. Logically, the processing of hiding the secret information in the cover image is known as embedding.

**Payload:** The information which is to be concealed. The information to be hidden in the cover data is known as the "embedded" data.

**Secret key:** This is the key used as a password to encrypt and decrypt the cover and stego respectively in order to extract the hidden message. Secret key is optional.

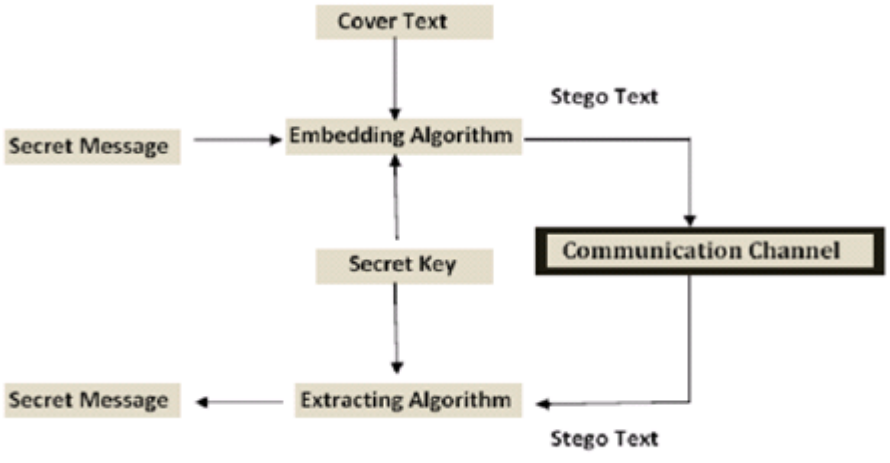



Fig-1

**COVER IMAGE + MESSAGE ⟶ STEGOIMAGE**

**+ " SOURAV "**

**(TEXT BE HIDDEN IN THE IMAGE)**

Fig-2

Here,we have used cover image as an uint8 image and the secret message as "SOURAV" which is to be hidden in the image.In this block diagram, we have used the LSB algorithm to hide a text message in an image.As we can see that the stegoimage which we obtained after the LSB algorithm been applied ,is very much similar to the cover image.In other words,the property of the cover image does not change significantly.

## 2. LITERACY SURVEY

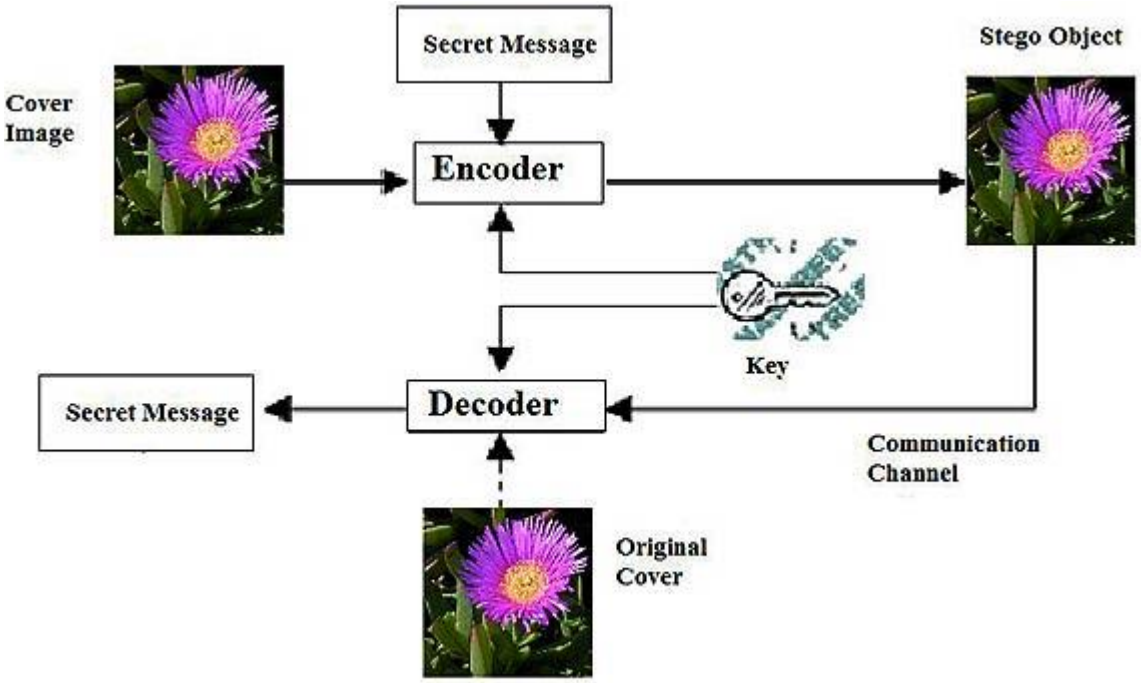



**Fig-3 Block Diagram of Steganography**

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The Steganography system which uses

an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography. The LSB is the lowest significant bit in the byte value of the image pixel. The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image.

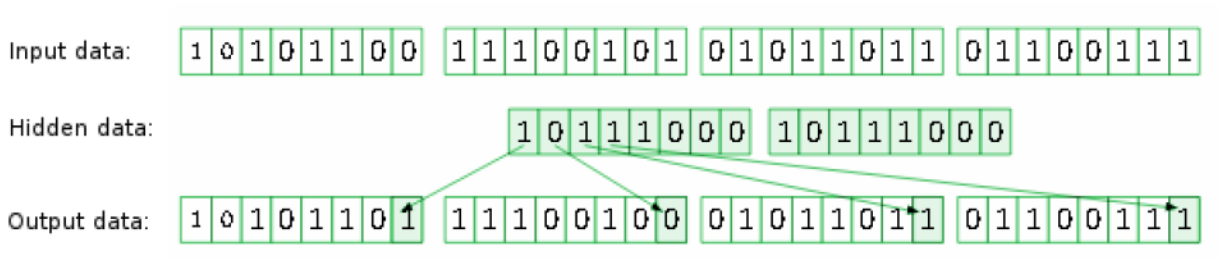



FIG-4

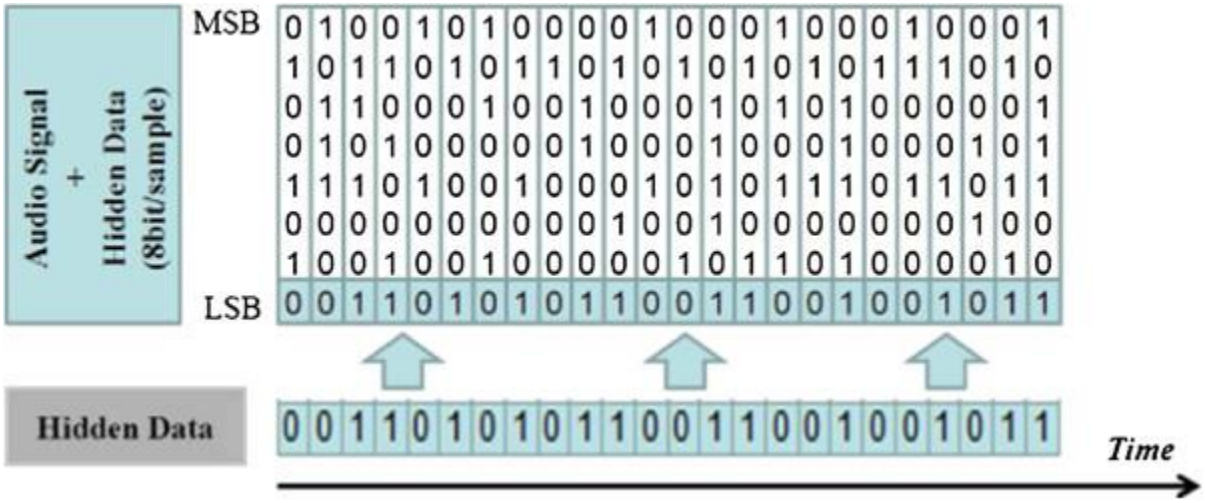



FIG-5 **AUDIO STEGANOGRAPHY**

Incase of Audio Steganography, each sample of audio Signal contains 8bits, so here also we can hide any secret message by placing the message signal bits in the LSB of each sample of audio signal.In this way we can achieve Audio Steganography.

In Image Steganography, we have used two uint8 images where each pixel contains 8 bits. One image is called as Message image which is to be hided and another image is known as the Cover Image where the message image needs to be hided. Here in the Embedding Algorithm, at first the cover image gets bitwise complemented then it is Bitwise Anded with its complement. Then Bit-Wise Right Shift operation of the Message Image with the number of bits Entered by the User takes place and finally Bit-Wise OR Operation Cover Image and Message Image would give the final Stego image.

Cover Image

Fig-6

Message Image

Fig-7

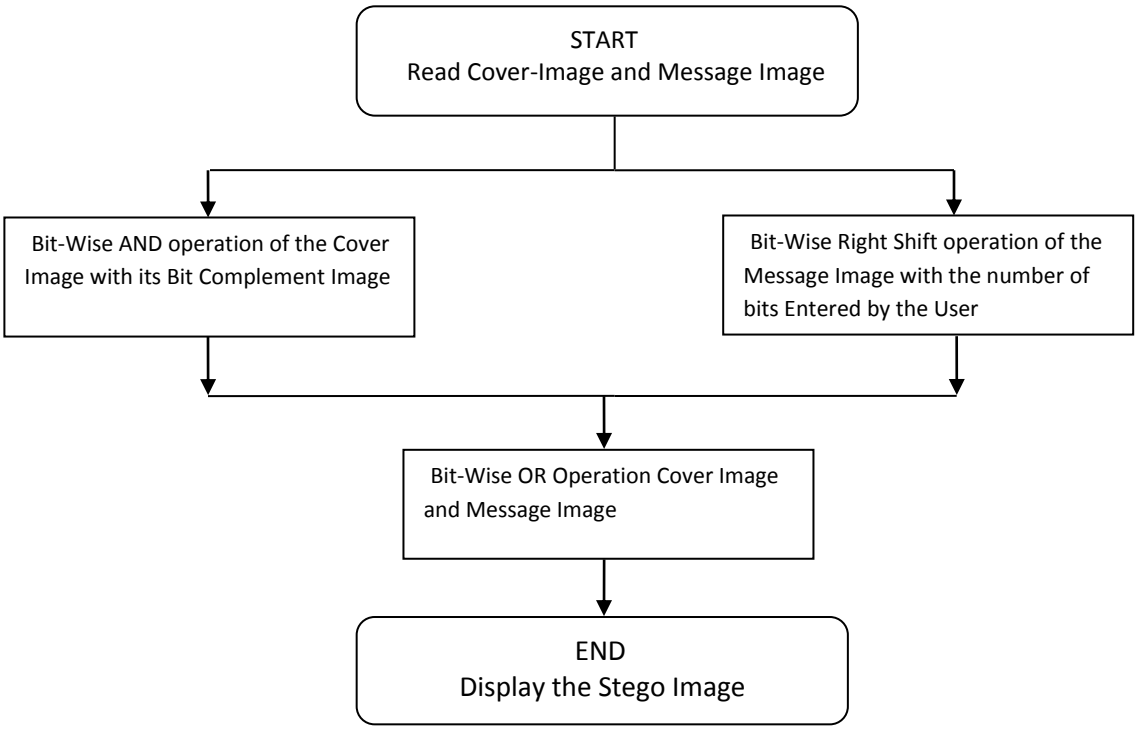
Here, uint8 Stego Image is obtained by the LSB substitution of Message image bits in the uint8 Cover Image and then the Extracted image is obtained from the Stego Image with the help of below mentioned algorithm.

Stego image

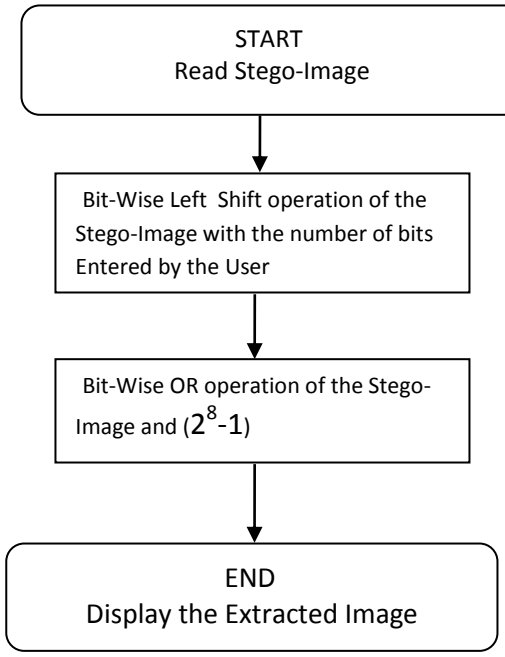
Extracted image

Fig-8 NUMBER OF LSB BITS SUBSTITUTED = 1

## FLOW-CHART OF THE EMBEDDING ALGORITHM USED




## FLOW-CHART OF THE EXTRACTION ALGORITHM USED



In the Extraction Process, Stego Image is first Bit-Wise Left Shifted with the number of bits Entered by the User and then Stego-Image is Bit-Wise ORed with ($2^8$-1). In this way Original Message Image is obtained from the Stego-Image. In Mat lab we have implemented this logic and obtained different Extracted Images from different Stego-Images under conditions of Different LSB bits substituted.

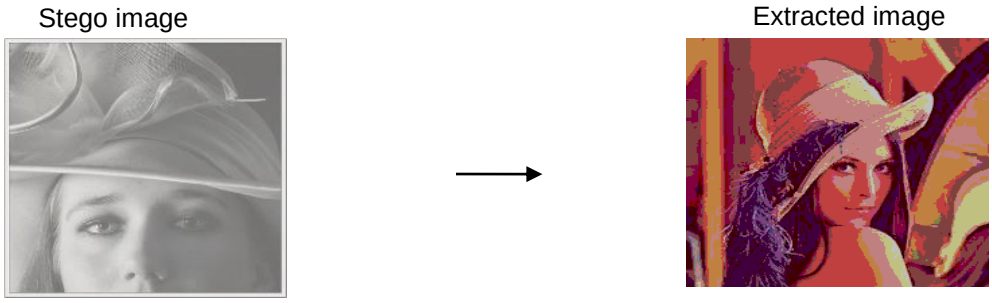



Fig-9 NUMBER OF LSB BITS SUBSTITUTED = 2

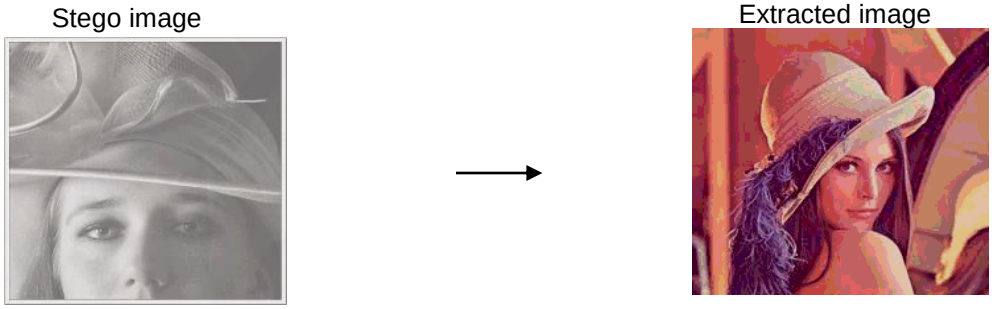



Fig-10 NUMBER OF LSB BITS SUBSTITUTED = 3

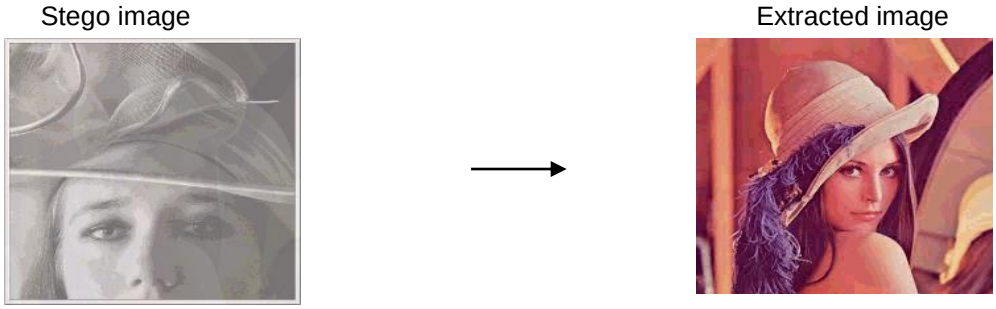



Fig-11 NUMBER OF LSB BITS SUBSTITUTED = 4

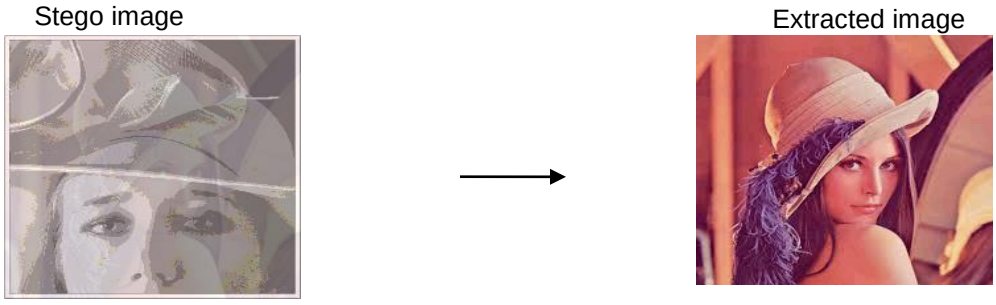



Fig-12 NUMBER OF LSB BITS SUBSTITUTED = 5

## 3. RESULTS AND INTERPRETATIONS

Here, we have computed the PSNR values and MSE for different LSB Bit Substitutions and we found that if we increase the number of LSB Bit Substitutions from 1 to 5, PSNR value will increase and the MSE value will decrease. As we know PSNR value is inversely proportional to MSE, so with decrease in MSE will make sure that PSNR value should decrease. In this paper, we have kept on substituting the LSB bits up to 5 since after that Stego Image will no longer look like the cover image.

TABLE-1

| NO. OF LSB-BITS SUBSTITUTED | PSNR VALUE(db) | MSE VALUE |
|---|---|---|
| 1 | 24.3468 | 239.0038 |
| 2 | 24.8948 | 210.6692 |
| 3 | 25.9503 | 165.2140 |
| 4 | 29.1256 | 79.5280 |
| 5 | 35.6974 | 17.5123 |

## 4. CONCLUSION

In Recent years, we have seen after going through different research papers that no algorithm is suitable for all types of Steganography.One Algorithm that is suitable for Text steganography may not be suitable for Image steganography. However, in this paper, we have compared different Sego-images which are obtained from different number of LSB-Bit substitutions and computed the PSNR values and MSE values from each Stego-Images. By comparing the different Stego images we have found that if we increase the number of LSB Bit Substitutions, the Stego-image will no longer look like the original Cover Image. In other words Cover Image changes as we increase the LSB Bit substitution.

## REFERENCES

1. Ian T. Young, Jan J. Gerbrands, Lucas J. van Vliet," Fundamentals of Image processing".

2. Rafael C. Gonzalez, Richard E. Woods," Digital Image Processing 3rd edition"

3. Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999
4. Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*, 47:10, October 2004

5. Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001

6. Johnson, N.F. & Jajodia, S., "Steganalysis of Images Created Using Current Steganography Software", *Proceedings of the 2nd Information Hiding Workshop*, April 1998
7. Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", *IEEE Security and Privacy Journal*, 2003

8. M. Pavani1, S. Naganjaneyulu, C. Nagaraju, "A Survey on LSB Based Steganography Methods" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467

9. Stuti Goel, Arun Rana, Manpreet Kaur,"A Review of Comparison Techniques of Image Steganography", IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48

10. Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999