International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com

ISSN No: 2456 - 6470 | Volume - 3 | Issue – 1 | Nov – Dec 2018

LSB Based Image Steganography for Information Security System

Aung Myint Aye
Professor, University of Computer Studies, Loikaw,
Kayah State, Republic of the Union of Myanmar, Myanmar

ABSTRACT

Information hiding in a cover file is one of the most modernized and effective ways for transferring secret message from sender to receiver over the communication channel. There are many steganographic techniques for hiding secret message in image, text, audio, video and so on. Image Steganography is also one of the common methods used for hiding the information in the cover image. In this research work, the secret message is hidden in a cover image file using image steganography. LSB is very efficient algorithm used to embed the information in a cover file. The LSB based image steganography with various file sizes is analyzed and illustrated their results. Bitmap (*.bmp) image is used as a cover image file to implement the proposed system. The detail Least Significant Bit (LSB) based image steganography is introduced. In this paper, the new embedding algorithm and extracting algorithm are presented. While embedding the secret message in a cover image file, the starting embedded pixel is chosen according to public shared key between sender and receiver. The original cover image and embedded image with secret message are analyzed with PSNR values and SNR values to achieve security. The resulting embedded image shows the acceptable PSNR and SNR values while comparing with the original cover image. The proposed system can help the information exchanging system over communication media.

Keywords: *Image Steganography, LSB, Data hiding, information security, PSNR*

I. INTRODUCTION:

Significant advancements in digital imaging during the last decade have added a few innovative dimensions to the field of image processing [1]. The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing [2]. In image steganography the information is hidden exclusively in images. It is one of the effective means of data hiding that protects data from unauthorized or unwanted disclosure and can be used in various field such as medicines, research, defense and intelligence for secret data storage, confidential communication, protection of data from alteration and disclosure and access control in digital distribution.

The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message, it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data [2]. The image obtained after insertion of message is called a stego image. Insertion of secret message is done in Least Significant Bit (LSB) of the image pixels in this paper. Then the stego image formed is having a message which is invisible to human eye. This means that one cannot find the difference between the original image and stego image. The secret message is inserted by using an algorithm and the secret message is obtained from stego image by using reverse algorithm [4].

The organization and implementation of the paper is as follows. The following section presents the process of Steganography. Then experimental results are expressed and discussion and conclusion are at the end.

II. STEGANOGRAPHY

Steganography is a process of secret communication where a piece of information (a secret message) is hidden into another piece of innocent looking information, called a cover. The message is hidden inside the cover in such a way that the very existence of the secret information in the cover cannot be estimated in any suspicion in the minds of the viewers

[1]. Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography plays an important role in information security. It is the art of invisible communication by concealing information inside other information.

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 (CVR) [7]. One of the common techniques is based on manipulating Least Significant Bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity [6]. LSB substitution is also the process of adjusting the least significant bit pixels of the carrier image [8].

The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB technique, just four bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same.

III. LEAST SIGNIFICANT BIT (LSB) TECHNIQUE

In Least Significant Bit Algorithm, both secret message and the cover image are firstly converted from their pixel format to binary. And the Least Significant Bit of the image is substituted with the bit of the secret message to be transferred so as to reflect the message that needs to be hidden. The bits of the secret message replace each of the colors of the Least Significant Bit of the Image [9]. Every pixel in an image indicates a color and, the each image is made up of pixels [5].

The right-most value is the LSB value of related image pixel sequence. If the LSB is a 1, then the total will be an odd number, and if 0, it will be an even number. However, changing the LSB value from a 0 to a 1 does not have a huge impact on the final result. Each 8-bit binary sequence is used for expressing the color of a pixel for an image, so changing the LSB value from a 0 to 1 does not impose a major change and it is unlikely to be noticed by an observer. In fact, the LSBs of each pixel value could be potentially modified, and the changes would still not be visible. This provides an enormous amount of redundancy in the image data, which means that we can effectively substitute the LSBs of the image data, with each bit of the message data until the entire message has been embedded. This is meant by Least Significant Bit Substitution Method.

One of the earliest stego-systems to surface was those referred to as Least Significant Bit Substitution techniques, socalled because of how the message data is embedded within a cover image c. In computer science, the term Least Significant Bit (LSB) refers to the smallest (right-most) bit of a binary sequence. The structure of binary is such that each integer may only be either a 0 or a 1, often thought of as off and on respectively. Starting from the right, the value (if on) denotes a 1. The value to its left (if on) denotes a 2, and so on where the values double each time.

This value essentially determines whether the total sum is odd or even. If the LSB is a 1, then the total will be an odd number, and if 0, it will be an even number. However, changing the LSB value from a 0 to a 1 does not have a huge impact on the final figure; it will only ever change by +1 at most. If we now think of each 8-bit binary sequence as a means of expressing the colour of a pixel for an image, it should be clear to see that changing the LSB value from a 0 to a 1 will only change the colour by +1 - a change that is unlikely to be noticed with the naked eye. In fact, the LSBs of each pixel value could potentially be modified, and the changes would still not be visible. This highlights a huge amount of redundancy in the image data, and means that we can effectively substitute the LSBs of the image data, with each bit of the message data until the entire message has been embedded. This is meant by Least Significant Bit Substitution. Now if the message is embedded as is into LSB of the cover image, then the resultant structure in the LSB plane of the stego-image would clearly be a giveaway [3]. The embedding algorithm at the sender side and extracting algorithm at the receiver side are presented as follows:

A. The embedding algorithm at the sender side

Step (1) : Get the input cover image and secret message.
Step (2) : Accept the stego-key from the user and calculate average value of them.
Step (3) : Convert each character of secret message and each LSB bit of cover image (R-channel) from the position of calculated average of stego-key.
Step (4) : Substitute the LSB bit of cover image (R-channel) with binary values of secret message with respect to the starting point until the end of secret message.
Step (5) : Insert the end character value at the end of secret message.
Step (6) : Calculate the PSNR, SNR of original and resulting images.
Step (7) : Send a stego-image to the receiver.

B. The extracting algorithm at the receiver side

Step (1) : Get the input stego-key from the userand calculate average value of them.
Step (2) : Load the stego-image that is sent from the sender.
Step (3) : Extract each of LSB bit from the stego-image until to find out the end bit.
Step (4) : Reconstruct the collecting LSB bits from the stego-image.
Step (5) : Transform the LSB bits to correspondent characters.

IV. IMPLEMENTATION OF PROPOSED SYSTEM

In this proposed system, the secret message is used to hide in a cover bmp image. Firstly each character of secret message and each pixel of cover bmp image are converted into binary values. The user has to input stego-key as the password of stego-key is used to embed the secret message in a cover file.

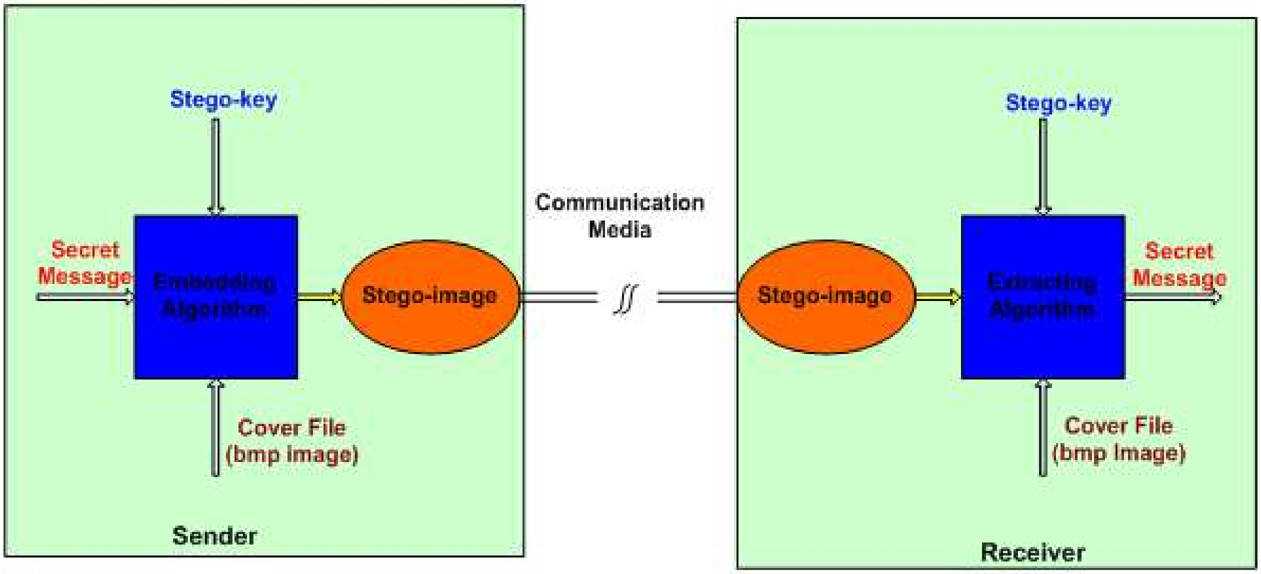


Figure1. Overview of proposed system

After inserting secret message into cover image file, the resulting stego-image is sent to the receiver through the desired communication channel. The above figure 1 shows the overall system design of proposed system.

While inserting a binary bit of secret message into cover image, each pixel value of cover image, which is in decimal in value, is converted into binary values as shown in figure 2. In this case, there are R, G, B channel values of each pixel of cover image, but only the R-channge LSB bit values are used to substitute. Similarly each character of secret message is converted from decimal value to binary value. Finally the converted binary value of secret message is substituted into each LSB bit of R-channel of cover image until the end of secret message. In this case the starting substitution point is chosen according to the input stego-key. The figure 3 illustrates the substitution of secret message into each LSB bit of cover image.

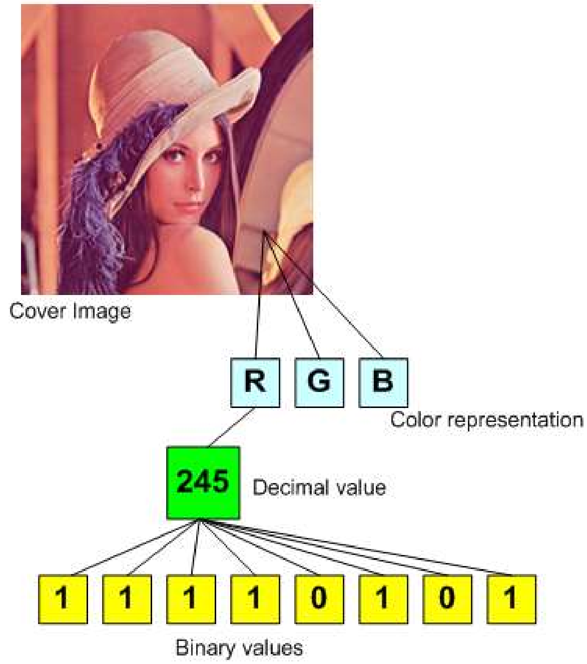


Figure2. Pixel representation and binary values

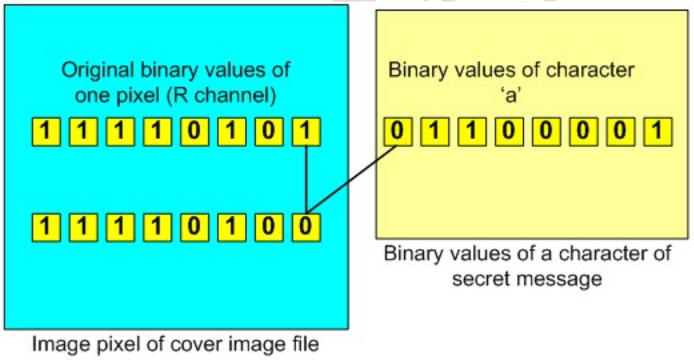
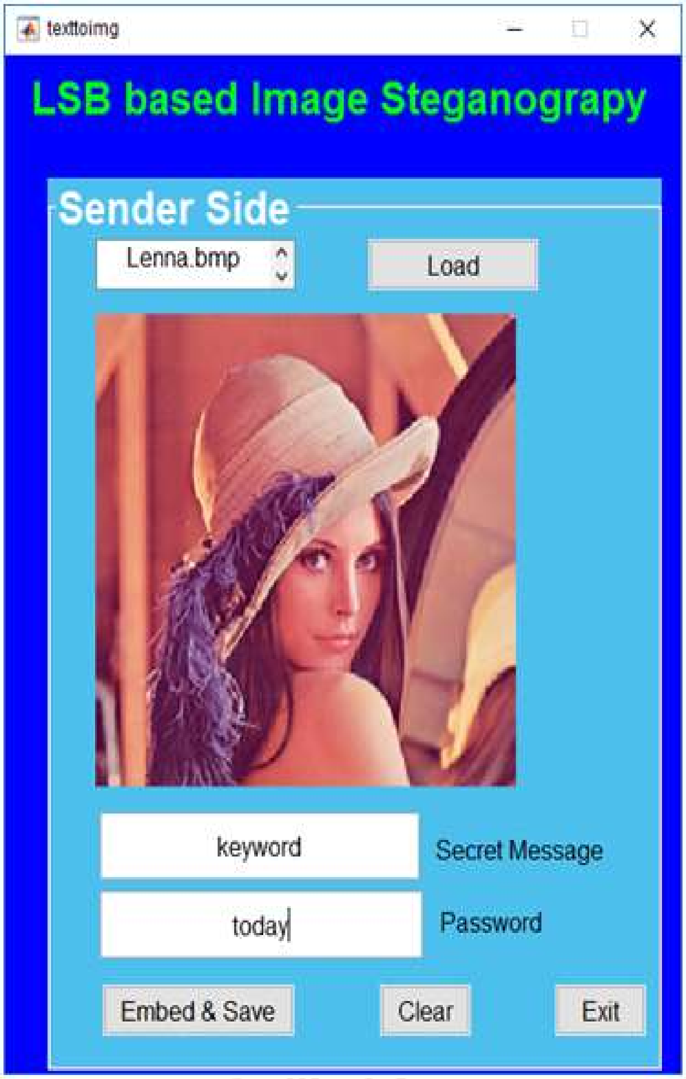

Original binary values of one pixel (R channel)
1 1 1 1 0 1 0 1
1 1 1 1 0 1 0 0
Image pixel of cover image file
Binary values of character 'a'
0 1 1 0 0 0 0 1
Binary values of a character of secret message

Figure 3.LSB substitution algorithm of proposed system

While defining the starting point of embedding LSB, the stego-key is firstly collected from the user. The summation of the ASCII value of each character of stego-key is calculated and then the average of those characters value is computed. While substituting the secret message into LSB of cover image, the first LSB position is chosen according to the calculated average value of input stego-key characters. Then the substitution processing will continue until the end of secret message.

V. EXPERIMENTAL RESULTS AND ANALYSIS

The following figure 4 shows the required processes at the sender side, in this case, the user has to input the stego-key which is already shared with the receiver side. In this research work, the cover image type of bmp is used to evaluate.


texttoimg

LSB based Image Steganograpy

Sender Side

Lenna.bmp

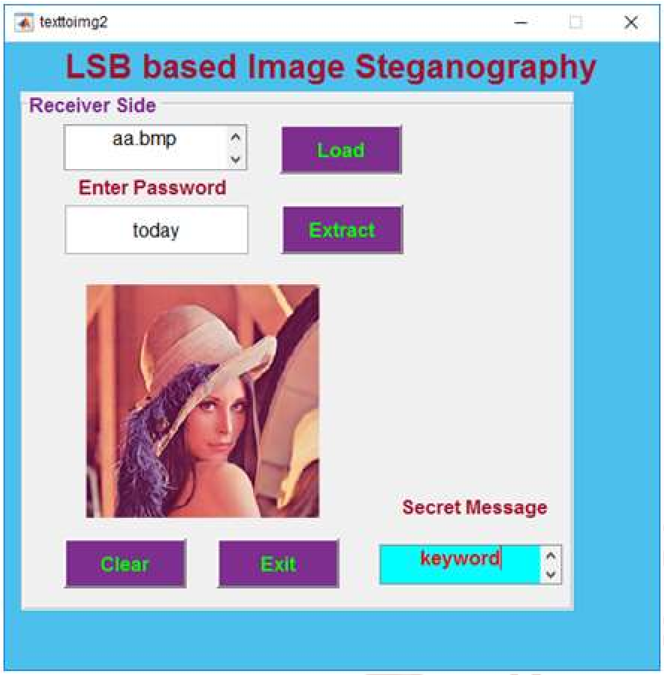
Secret Message: keyword

Password: today

Figure 4.Sender side of proposed system

There are three portions at the sender side to accept as shown in figure 4.The first one is choosing the input cover image file, and then inputting the desired secret message and finally stego-key. The stego-key is very important to substitute and to extract secret message at both sides. The secret message should be arbitrary, the size of secret message can increase the processing time of substitution into the cover image.

The following figure 5 shows the overall processes at the receiver side. The first important one is stego-key which is used to evaluate the average value of input characters. After calculating the average of input characters, the proposed system can point out the starting point to extract the secret message. The second important one is the sent stego-image which must be in bmp file format only. Finally the proposed system can successfully extract the original secret message with correct stego-key.



aa.bmp

today

keyword

Figure5. Receiver side of proposed system

When the proposed system evaluates, the original cover image is changed according to the input secret message and stego-key. The PSNR and SNR values of original and resulting images are calculated and compared in the following table 1. The resulting PSNR and SNR values of substituted cover image show a little bit changes with the original ones. In this case, different six bmp cover images are used to implement the proposed system.

In order to measure the performance of the image compression algorithms two performance parameters are used in this system.

- Signal to Noise Ratio (SNR)
- Peak Signal to Noise Ratio (PSNR)

A. Signal to Noise Ratio

The signal to noise ratio (SNR) is a technical term used to characterize the quality of the signal detection of a measuring system. In this case, a system uses a noise “salt and pepper” with the original cover images.

B. Peak Signal to Noise Ratio (PSNR)

Mean Squared Error (MSE) is defined as the square of differences in the pixel values between the corresponding pixels of the two images. The mean square error (MSE) of N * M size image is given by the following equation (1),

$$MSE= \Sigma M, N\ [I1\ (m, n) - I2\ (m, n)]\ 2\ /\ (M*N) \qquad (1)$$

M &N -number of rows and columns in the input images.

PSNR (peak signal to noise ratio) -PSNR Peak signal-to-noise ratio often abbreviated PSNR, is an engineering name, for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity.

The peak error between the compressed image and original image is measured in terms of PSNR. The higher value of PSNR indicates higher quality of image. To calculate PSNR, MSE is first computed.

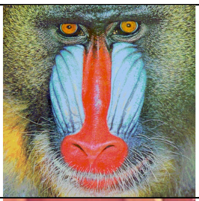
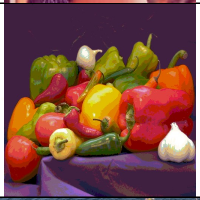
PSNR value can be derived as in equation (2). Here ‘O’ and ‘D’ are the original and the distorted image pixel values (binary), respectively, to be compared, and the image size is M x N.

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \qquad (2)$$

Here, *MAX* is the peak value of the pixels in an image. *MAX* is 255 when pixels are presented in an 8-bitformat. Theoretically, the higher the PSNR value is, the better the image processing is; however, practically, there are some problems reported in the literature about the use of the PSNR for image quality assessment.

Table1. The comparison results of PSNR and SNR values between original and embedded images

No.	Types of Images	Original Image		Embedded Image		Image Size	Resulting Images
		PSNR	SNR	PSNR	SNR		
1	flower.bmp	22.2474	17.5806	22.2568	17.59	255x256	

2	mandrill.bmp	21.8341	16.6596	21.8459	16.67	512x512	
3	lenna.bmp	21.9866	16.8408	22.0123	16.87	220x220	
4	peppers.bmp	21.9163	12.4611	21.9112	12.46	512x512	
5	sails.bmp	21.9336	16.9037	22.0068	16.98	768x512	
6	boy.bmp	21.9816	17.1659	21.9232	17.11	768x512	

VI. DISCUSSION AND CONCLUSION

In this research work, proposed LSB based steganography for embedding and extracting algorithms are presented. LSB based steganography embed the text message in LSB of the pixels of cover image according to the input stego-key. This paper also compares the results of PSNR values and SNR values of original and resulting cover images. The main goal of this paper is to show how secret image can be embedded and how it can be sent through the internet by fooling grabbers.

Many problems can be encountered when important data is transferred over the public communication media. A safe and secure procedure is needed to transfer them easily. For this purpose simple image hiding techniques are used and the quality of stego images is also improved by using LSB substitution algorithms. So the hackers may not estimate secret message with resultingstego image. The experimental results show that the stego image and the cover image remain more or less identical which is the main focus of this paper. This means that a secret message can be sent to the destination without changes. Finally the PSNR and SNR values of original and embedded images are compared and analyzed. The comparison results show that the embedded resulting image is totally identical with the original ones.

As the further work, other color cover image types such as jpg, tiff, png and so on will be used to compare with those results. Another better embedding and extracting algorithms will be used to implement it. Also not only secret text message but also secret image or data will be used to embed in a cover file. It is expected to find better technique and algorithms to hide more data in a cover image.

Reference

1. M. Mishra, Department of Information and Communication Technology and Dr. M.C. Adhikary, Department of Applied Physics and Ballistics, “An Easy Yet Effective Method for Detecting Spatial Domain LSB Steganography”, International Journal of Computer Science and Business Informatics, vol.8, No.1 Dec 2013.
2. K. J. Devi, “A Secure Image Steganography using LSB Technique and Pseudo Random Encoding Technique”, Department of Computer Science and Engineering National Institute of Technology-Rourkela Odisha, Bachelor Thesis, May 2013.

3. R. Chandramouli, Msync lab, Stevens Institute of Technology, Dept. of Electrical and Computer Engineering, Hoboken and N. Memon, Polytechnic University, Computer Science Department, Brooklyn, "Analysis of LSB Based Image Steganography Techniques, IEEE 2001.

4. A. Khurana, Dept of Electronic, Punjab, India and B. M. Mehta, Dept of ECE, Punjab, India, "Comparison of LSB and MSB based Image Steganography, International Journal of Computer Science and Technology, Vol. 3 Issue 3, July-Sept 2012.

5. R. R. Krupa, Department of Information Technology, the Standard Fireworks, Rajaratnam College for Women, Sivakasi, Tamilnadu, India, "An Overview of Image Hiding Techniquess in Image Processing", The SIJ Transaction of Computer Science Engineering and its Applications (CSEA), Vol.2, No.2, March-April 2014.

6. C. Chan, Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong, "Hiding Data in Images by Simple LSB Substitution", the Journal of the Pattern Recognition Society, August 2003.

7. B, S. Champakamala, K. Padmini, K. D. Radhika, Department of TCE, Don Bosco Institute of Technology, Bangalore, India, "Least Significant Bit Algorithm for Image Steganography", International Journal of Advanced Computer Technology, Vol.3, No.4, August 2014.

8. C, R, Ravinder, A, R, Roja, Department of Master of Computer Appliccations, Teegala Krishna Reddy Engineering College, Medbowli, Meerpet, Hyderabad, "The Process of Encoding and Decoding of Image Steganography using LSB Algorithm", International Journal of Computer Science and Engineering Technology", Vol.2, Issue 11, Nov 2012.

9. 9. O. Osunade, and I. A. Ganiyu, Department of Computer Science, University of Ibadan, Ibadan, "Enhancing the Least Significant Bit (LSB) Algorithm for Steganography", International Journal of Computer Application, Vol. 149, No.3, Sept 2016.