© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

An Adequate Image Stegnography Method based on Bit Reversed Technique

A. Rakesh*, Dr. K. Kuppusamy
Department of Computer Science, Alagappa University, Karaikudi, Tamil Nadu, India

ABSTRACT

The concept of information hiding is nothing new inside the history, as early as in ancient Greece there have been tries to hide a message in a depended medium to deliver it across the enemy territory. Within the modern-day world of digital conversation, there are numerous techniques used for hiding information in any medium. Certainly one of such method is steganography [9] wherein digital media specifically digital pictures are used as a medium for hiding data and the facts within the shape text, virtual photograph, video or audio record may be used as secret message. The phrase steganography derived from two Greek words: steganos way covered and graphos approach writing and often refers to secret writing or facts hiding [10]. The main goal of steganography is to increase conversation protection via placing secret message into the virtual picture.In this paper Proposed the Least Significant bit (LSB) method is the simple steganographic technique to conceal the secret data in an image and it is commonly used. This method maintains the quality of the image. Steganography using LSB hides out the bits of the message image into the LSB of the cover image. The advantage of LSB steganography is that it is very simple, easy to employ and the final image obtained will be almost similar to the cover image, meaning that the quality of cover image remains same.

Keywords : Steganography, LSB Technique, Information Hiding, Secret Image, Cover Image.

I. INTRODUCTION

Steganography is a data hiding technique which disguises the presence of information in the source. Steganography furnishes hiding of text, images, audio, video etc to protect from attackers and make sure the message contained is kept secret. On the other side, cryptography is another form of hiding secret messages through encrypting the data contained in Images, texts, videos, audios etc. Also during steganography implanting the message in a cover image, the embedded message changes the original attributes of the image. Cryptography is mainly intended for attackers, where as steganography mainly focuses on hiding messages while transmission. For example, the master image file is referred as cover image and after implanting the secret message the image is referred to as stego-image. Once the stenography on the image is finished, then it is shared or transmitted to the other user.

Image steganography is a method which is utilized to conceal secret content within an image. The binary bits of secret information are concealed in the binary of image and this marginally impacts the magnitude of color and brightness which is difficult to detect for a human eye [1]. Several algorithms are used for image steganography, where some of them are complex and some of them are simple. In general images are the mostly used for steganography when compared to text, audio and video objects. Regarding digital images many dissimilar variety of formats are available and are used accordingly for particular applications. A simple image steganographic framework comprises an original image, called cover (I) image in which secret message image (M) is hidden or embedded along with

a stego key (K), the stego key applied to conceal the data as well as to draw out. The purpose of using stego key is to allow for protection [2]. The aim of cryptography and steganography is to offer hidden communication.

Substitution method is widely applied to exchange the least significant bits of data that influence the significant content of the original image with new data in a way that makes the least amount of deformation. Using this technique the cover image file size does not gets altered after the performance of the substitution. At the same time, this approach depends on the substitution bits, which limit the size of the information bits and the final stego-image, gets affected to an extent and may raise doubts.

Least Significant bit (LSB) method is the simple steganographic technique to conceal the secret data in an image and it is commonly used. This method maintains the quality of the image. Steganography using LSB hides out the bits of the message image into the LSB of the cover image. The advantage of LSB steganography is that it is very simple, easy to employ and the final image obtained will be almost similar to the cover image, meaning that the quality of cover image remains same.

In Section 2 gives brief the present work of this research describe the Least Significant Bit algorithm and the Bit Inversion technique. In Section 3 gives the Result and Discussions of this research work which describes the implementation of bit inversion technique in MATLAB with the performance analysis and screenshot display models are engraved in this chapter. Discussed in Section 4 summarizes the conclusion of the research work which gives the idea and concept of future scope to carry the research.

II. PROPOSED RESEARCH WORK

Digital images, videos, audio files, and other computer formats that contain surplus data information can be used as secret messages carriers. After embedding a secret message into the cover-image, then the image will be called stego-image, which does not hold any easily detectable changes. An intruder or a third party could use such changes as a suggestion that a secret message may be present. Steganographic technique becomes meaningless when the message is detected and read, also, when less information is attached into the cover-image, lesser the chance of detection. Another important feature of steganography is the choice of the cover-image, through which any person can choose any medium as his cover. The selection of cover medium is at the person who sends the hidden message.

The sender should always be careful in choosing cover medium, avoiding using cover-images that would be easy to establish the presence of secret messages can successfully send his message. For example, art, charts, images with uniform color, images with only a few colors, and images with a unique textual content, such as fonts can be easily interpreted. Although computer-generated forms or images may seem as good covers sources because computer generated are filled with complexity and irregularity. The medical field is one another industry that uses image in Steganography and the industry widely deals with images, exchanging between doctors and patients. These embedded images can store patient data and we can avoid additional storage system and privacy problems, example can be given for storing patients information in the x-ray itself.

For data streams there are several techniques used, the simplest method of Steganography is the “LSB Algorithm”. The principle of LSB method is embedding a secret message into a data. The procedure for such technique is to convert the desired

hidden message into binary form and then embedded each digit into a least significant bit of the data image. Most Significant Bit (MSB) embedding is a technique much similar of the Least Significant Bit Steganography. Same principle is used for exchanging the most significant bit of the taken image and exchanging it with the digits of the converted to binary form message.

In our proposed work, RGB pixel value based steganography method is proposed using LSB inversion techniques. The specialty of this method is that we does not substitute the picture element like other steganography methods, we use only LSB. All digital images are generally stored either in 24 bit or 8 bit known as Grayscale. A 24 bit picture offers the majority of space for concealing information; however it can make the file quite large meaning, the size of the stego image file becomes high. All color sequence is gained from three main colors namely red, blue and green, where every individual pixel of this basic color is made up by one byte.

The basic concept of steganography is that it has a cover object which is used to cover the original message image and becomes a host object with the message would be transmitted through the steganography algorithm to carry out hiding. The result of such steganography is an image called stego-image which has the message image inside it, hidden. This stego image is then broadcast to the receiver where the receiver recalls the hidden message image by utilizing de-steganography.

The Benefits of Least-Significant-Bit (LSB) steganographic data implanting are that it is easy, simple to understand, easy to implement, and it produces stego-image that is almost similar to cover image and its alterations not visible to naked eyes. Over the years, several steganography methods based on LSB have been proposed and implemented; a good steganographic technique should focus on three things, namely, capacity, visual quality and security. On the other hand simple LSB technique aims for one bit per pixel and generally it is good at visual quality but poor at the data capacity. This simple LSB suffers in terms of large data volume, which does not satisfy the three mentioned earlier, i.e. capacity, visual quality and security. On the other hand, the secret messages hidden can be easily retrieved through retrieving the LSB.

Our proposed method involves two main steps, we perform a plain LSB to understand the bit patterns of the 3rd and 4th bits of the Least significant bits and after which the bits (3rd and 4th) are reversed in order to make the steganalysis difficult to identify the changed bits in the 3rd and 4th pixel. The revering involves a specific bit-pattern that strengthens the LSB technique.

3.1 LEAST SIGNIFICANT BIT

The least significant bit of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types:

(i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the visual aspect of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden.

A raw digital image is an array of pixels constituting the chroma of light at that pixel position. Digital images are generally stored in either 24-bit or 8-bit per pixel. An 8-bit image can represent 256 different levels of light intensities. 24-bit images are sometimes known as true color images because they can represent a large number of color intensities. Obviously, a 24-bit image provides more space for

hiding information; however, 24-bit images are generally large and not that common. A 24-bit image is 1024 pixels wide by 768 pixels high would have a size in excess of 2 megabytes. As such, large files would pull attention when they were transmitted across a network. In general 8 bits images are used to hide information such as GIF files represented as a single byte for each pixel. Now, each pixel can correspond to 256 colors. It can be said that pixel value ranges from 0 to 255 and the selected pixels indicates certain colors on the screen. The technique for classical least significant bit involves the handling of LSB plane of cover image by replacing LSBs of cover image with message bits. Since only LSB is changed, only one level of intensity differs between original and modified pixel, which cannot be detected visually. Hence the attacker will not get the idea that some message is hidden in the image.

The disadvantages of LSB approach is the size of cover image required for a particular message image that is for a certain capacity of message cover image required is 8 times, this would increase the bandwidth to send the image and it creates suspicious on the file to look over. Another disadvantage is that if an attacker suspects that some information is hidden behind the cover image, He can easily extract information by just collecting LSBs of stego image. For these criteria, this method is not implemented in plain context but together with other encryption techniques.

For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are:
(11101010 11101000 11001011)

(01100110 11001010 11101000)
(11001001 00100101 11101001)
A steganographic program could hide the letter "J" which has a position 74 into ASCII character set and have a binary representation "01001010", by altering the channel bits of pixels.
(11101010 11101001 11001010)
(01100110 11001011 11101000)
(11001001 00100100 11101001)

In this case, only four bits needed to be changed to insert the character successfully. The resulting changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden. The advantage of LSB embedding is its simplicity and many techniques use these methods.

3.2 BIT INVERSION TECHNIQUE

A LSB bit inversion technique is used to inverse the last bit of each pixel in the cover image depending on the secret data.

a. Conversion of image to matrix

In the conversion process of image to matrix we convert the input cover image into matrix values. Initially the original image is in the RGB format which is then converted into grey scale image. The grey image is resized to a particular size of 256*256. Each image has intensity values for every pixel, here these intensity values are stored into a matrix.

b. Embedding process

Once image to matrix is completed the next step is involves embedding a image into an image. We use 3 and 4 bits inversions of an 8 bit images. The image obtained during this process is called as stegano-embed image. The secret image is embedded into the intensity values of image obtained during image to matrix conversion.

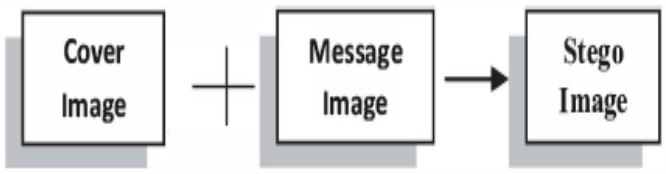
c. Conversion of matrix to image

In this step the intensity values of the images are converted back to image from the matrix. The image obtained has message embedded into it. The cover image and the image obtained here have to be

identical. Hence the objective of Steganography is satisfied.

d. Extraction process

The extraction process involves reading a pixel from the matrix array. Extract the LSB and replace the i^{th} bit in the message byte. By repeating the extraction on all bytes, the message image can be extracted. The output is interpreted with the PSNR and MSE values obtained



A. Embedding Message

B. Extraction Message

Fig 3.1 LSB Technique

3.3 METHODOLOGY

The proposed bit inversion technique is obtained by comparing the 2nd and 3rd bit from last, of the cover image to the bits from the stego image obtained from the basic LSB method. The process of the proposed method:

- ✓ Calculate the pattern instances of three bits on the cover-image. Classify the cover image according to number of patterns from 3 bits.
- ✓ Implement the basic LSB method to get the stego image.
- ✓ Once again from the stego image, calculate the pattern of instance in the 2nd and 3rd last bit of the stego-image.
- ✓ Match the similarity between for each pattern from cover image with the similar combination in the stego-image.
- ✓ Reverse the LSB bits with the number of pixels that have been altered is larger than the number of pixel that are not altered.
- ✓ Stock the position of the patterns that are substituted its pixel in a particular location. The flowchart of the proposed research work is given in fig 3.2

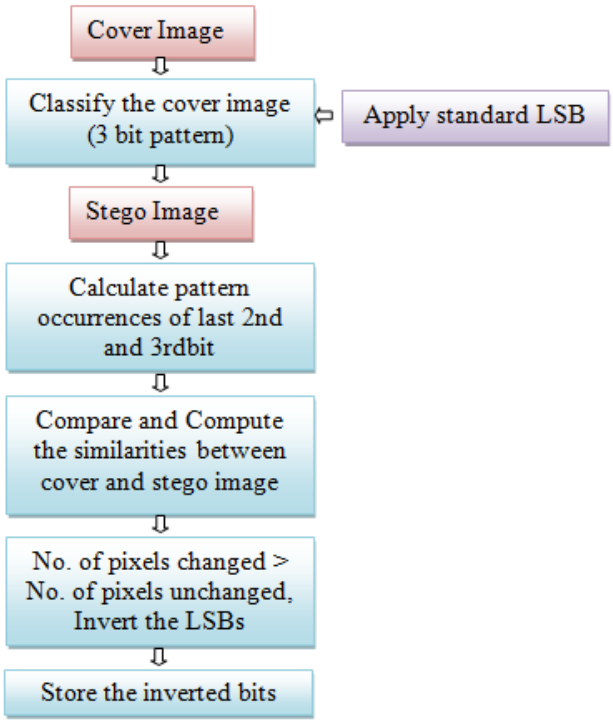


Fig 3.2 Flowchart of proposed work

Let us consider an example step by step to understand:

Secret message: 10011

Cover images	:10001100	10101101
	A	B
	10101011	1010110
	C	D
LSB		
stego-image :	10001**101**	10101**110**
	A	B
	10101**011**	10101**101**
	C	D

The four message bits from secret message 1 0 1 1 are to be hidden into four cover image pixels 10001100, 10101101, 10101011and 10101110. After simple LSB steganography, stego-image pixels are 10001**101**, 10101**110**, 10101**011** and 10101**101**. The first and second of cover image pixels have changed. Now, we can observer that the second and third LSB of cover image pixels are found to be 0 and 1 respectively. For these three combination pixels of two, LSB has changed. If we invert the LSB of these three pixels, cover picture pixels will be 10001100, 1010 1101, 10101011 and 10101100. At present, only one pixel is left in stego-image that differs from cover image i.e. the last second. Thus, replacing one pixel value does not alter the PSNR value and provides an increase in PSNR value through improving the image quality of stego-image. Towards right extraction of the message, we require to arrange the information that we have reversed the LSBs of those bits where the second and third LS Bits are 0 and 1 respectively.

For these message bits 10011, if we take three bits, there are minimum of five potential combination types. For each of the patterns (100,001,101,011,110), the stego image is examined to determine the number of bits of first type i.e. whose LS Bits has varied and continuing the process for second pattern type i.e. those patterns has not altered. When the number of bits of first pattern is larger than the number of second type bits, we reverse the LSB of first pattern type bits. In this manner, lesser amount of bits of cover image can be modified. The total bit gain would be equal to the difference between the number of first and second pattern bits.

When extracting the message, we need to stack those combination of patterns for which the matching LSB bit has been inverted, because we have assured through all possible patterns of 5 from 2^{nd} and 3^{rd} LS Bits and we require storing maximum of 5 patterns. While extracting the message from stego-image, there is a need to analyze 3^{rd}, 2^{nd} and 1^{st} LSB. The 2nd and 3rd LS Bits pattern in stego-image would be similar to that of original cover image, but only thing is the LS Bits has changed. To check for the stego-image pattern, the extractor must need the original image to get the message image.

Further to 2^{nd} and 3^{rd} LSB of each pixel, we also consider the least significant bit of the original image pixel. For each possible combination of 2nd and 3rd LSB, we find four types of pixels. First, the number of pixels in which the LSB has changed from 0 to 1. Second, the number of pixels in which the LSB is originally 0 and it hasn't changed. Third, the number of pixels in which the LSB has changed from 1 to O. fourth, the number of pixels in which the LSB is originally 1 and it hasn't changed. Let us denote these pixels by A, B, C and D respectively. Now, if A is greater than B, we invert the LSB in all those pixels that have the particular pattern of 2^{nd} and 3^{rd} LSB and LSB of those cover image pixels is originally O. Similarly, if C is greater than D, we also invert the LSB of all those pixels that have the particular pattern of 2^{nd} and 3^{rd} LSB and LSB of those cover image pixels is originally 1. In this way, less number of cover image pixels would be modified. Here, pixel benefit would be equal to min (A,B)+min(C,D). For de-steganography, we need to store those patterns for which the corresponding LSB bit has been inverted. As we have checked all possible combination (4) of 2nd and 3rd LSB and the LSB (0 or 1) itself, we may need to store maximum of 8 patterns. To recover the message image from stego-image, we need to analyze 3^{rd}, 2^{nd} and 1^{st} LSB. 2^{nd} and 3^{rd} LSB pattern in stego-image is same as in the original cover image, but LSB has changed. So, the receiver must have the original cover image for correct de-steganography. Similarly we repeat the bit inversion for up to 4 bits of the cover image utilizing maximum least significant bits.

III. RESULTS AND DISCUSSIONS

MATLAB is a high-performance programming language for technical computing. Matlab function is an easy to use; the interface function guides any user through the process of either encoding & decoding a message into or from the image respectively. In our study, Matlab is used for building bit inversion LSB steganography technique on the selected images.

4.1 Experimental Setup

The experiment is done using a set of 5 images with 256 x 256 dimensions. The bit inversion using LSB technique was developed in Matlab 2013. We use cover image of bird.png, flower.png and elephant.png. For secret images we use land.png and twinbird.png. The histogram analysis and PSNR and MSE values are used for interpretation. First we start experiment by inverting the LSB of 1 and gradually increased to 2, 3 and 4.

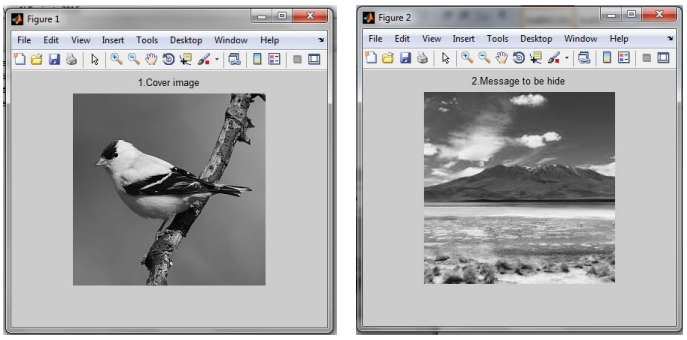
Cover Images : Bird Flower Elephant

Message Images : Land Twinbirds

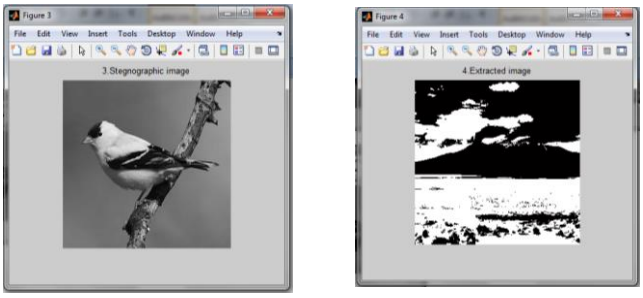
Fig 4.1 Images used in the experiment

4.2 EXPERIMENTAL RESULTS

a. LSB on 1 bits



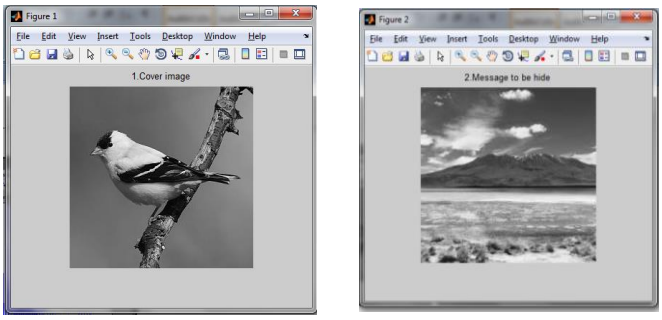
(a) (b)



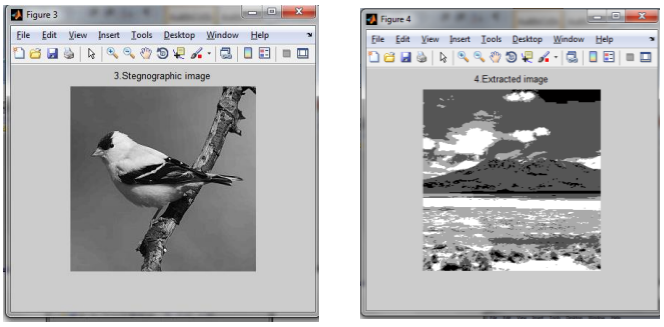
(c) (d)

Fig 4.2 1 Bit inversion LSB - Bird.png
a) Cover image b) Message image c) Stego image
d) Extracted image

b. LSB on 2 Bit



(a) (b)

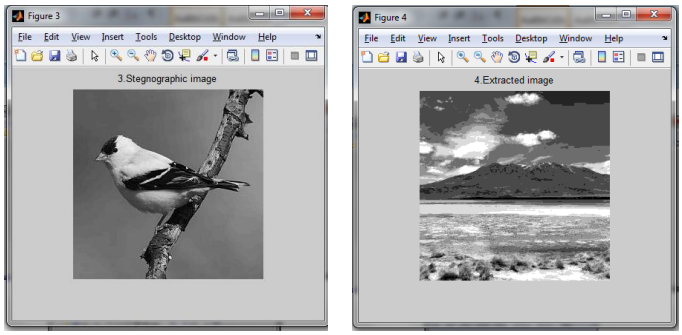


(c) (d)

Fig 4.3 2 Bit inversion LSB - Bird.png
a) Cover image b) Message image c) Stego image
d) Extracted image

c. LSB on 3 bits

(a) (b)

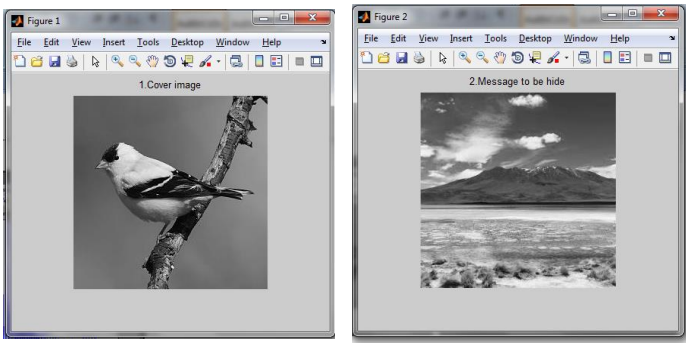


(c) (d)

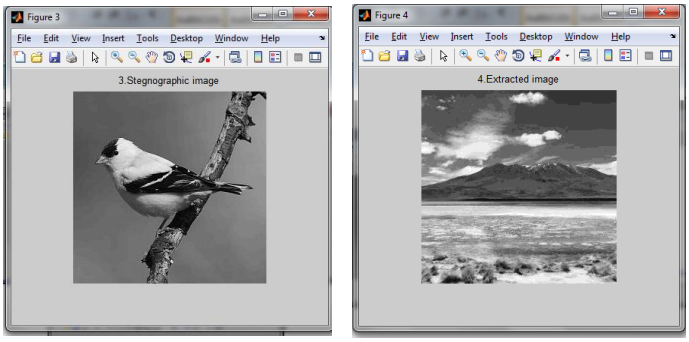
Fig 4.4 3 bit inversion LSB - Bird.png

a) Cover image b) Message image c) Stego image
d) Extracted image

d. LSB on 4 bits

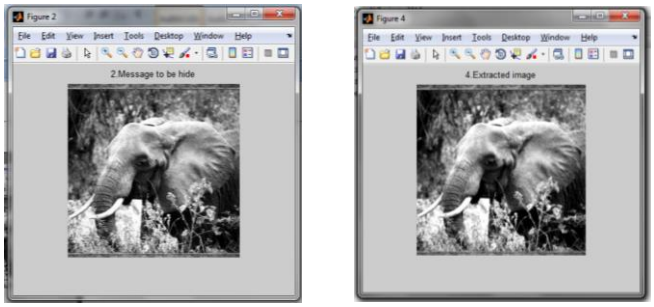


(a) (b)



(c) (d)

Fig 4.5 4 Bit inversion LSB - Bird.png
a) Cover image b) Message image c) Stego image
d) Extracted image



(a) Message image (b) Extracted image

Fig 4.6 Bit inversion LSB - Elephant.png

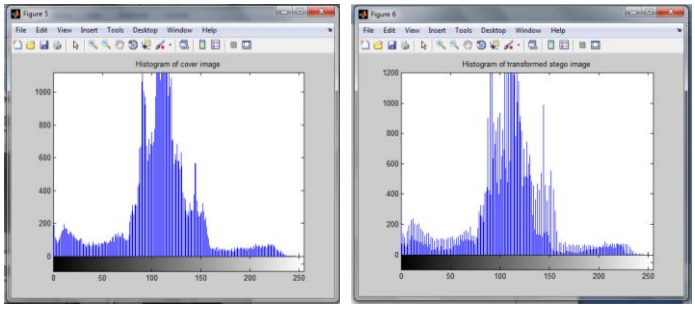
4.3 PERFORMANCE ANALYSIS

4.3.1 Histogram

In an image processing context, the histogram commonly refers to intensity of pixel values of an image. This histogram is a graph showing the number

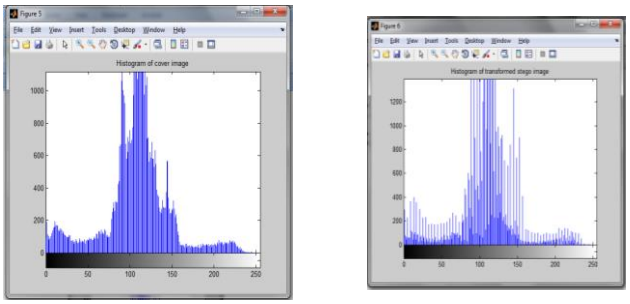
of pixels in an image at each different intensity value found on that image. For an 8-bit grayscale image there are 256 different possible intensities, and so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those grayscale values. Histograms can also be plotted for color images, either individual histograms of red, green and blue channels can be taken, or a 3-D histogram can be produced, with the three axes representing the red, blue and green channels, and brightness at each point representing the pixel count. The quality of the histogram differs with techniques and the intensity of the image used. Using histogram we can do pattern matching, inspect an element, color inspection and color matching.

The bird.png image is taken as cover image which has 256x256 pixel and land.png as message image with 256x256 pixel. The LSB bit inversion technique developed in Matlab, at first initiated the bit inversion from 1 bits and gradually increased the no of bit to 4. The histogram analysis of bird.png image is shown in fig 4.6 and the histogram analysis of elephant.png image is shown in fig 4.7.



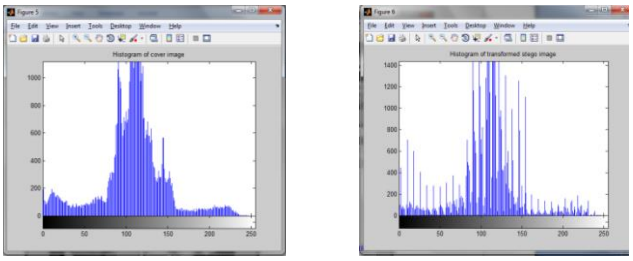
(a) Histogram of cover image (b) Histogram of stego image

Fig.4.7 Histogram of 1 bits inversion LSB



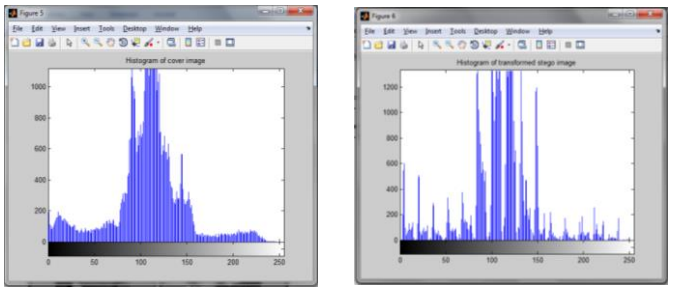
(a) Histogram of cover image (b) Histogram of transformed image

Fig 4.8 Histogram of 2 bit inversion LSB



(a) Histogram of cover image (b) Histogram of stego image

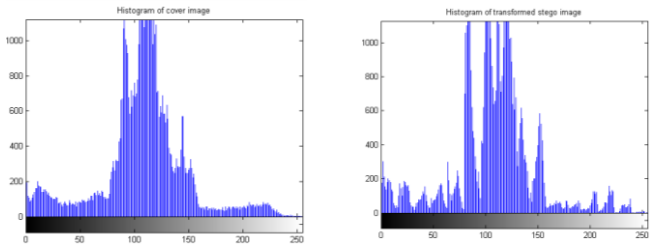
Fig 4.9 Histogram of 3 bits inversion LSB



Histogram of cover image Histogram of stego image

Fig 4.10 4 bits inversion LSB

4.11 Histogram analysis of Bird.png



Histogram of Cover image Histogram of Stego image

Fig 4.12 Histogram analysis of elephant.png

4.3.2 Peak Signal-to-Noise Ratio (PSNR)

PSNR is the standard measurement to test the quality of stego image in image steganography. PSNR is the ratio that lies between the power of a signal (cover image) and the power of noise (error) that affects the representation of an image. For example let us consider a cover image C of size N x N and the stego image of size M x M. Then, each cover image and stego image will have pixel values (x,y) ranges from (0 - N-1) and (0 - M-1).

$$\text{PSNR} = 10 \log_{10} \frac{\text{MAX}^2}{\text{MSE}} (\text{db}) \quad (1)$$

4.3.3 Mean Square Error (MSE)

The Mean Square Error (MSE) measures the average squares of the errors. Any measure of the center of a distribution should be associated with some measure of error. If we say that a number is a good measure of center, then most probably we are saying that it represents the entire distribution better, in some way, than other numbers.

Where $\text{MSE} = \frac{1}{\text{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (a_{i,j} - b_{i,j})^2$

The quality of the PSNR value determines the quality of the image, PSNR values below 30 db reflects low quality meaning that the image has undergone distortion due to embedding; greater than 40 db reflects that the image is not distorted.

The PSNR value and MSE value is calculated for bird.png image and is given in table 4.1.

Table 4.1 PSNR and MSE value of Bird.png

Image	1bit	2 bits	3 bits	4 bits
PSNR Value	34.9372	36.9851	39.6532	42.5978
MSE value	6.1386	4.7908	4.3815	3.5752

Take bird.png image as cover image which is 256x256 pixel and land.png as message image which is also 256x256 pixel. We apply LSB bit inversion technique developed in Matlab, at first we initiated the bit inversion from 1 bits and gradually increased the no of bit to 4. The Results are five below, the bit inversion for 1 bits lsb has a PSNR value of 34.9372 and MSE value of 6.1386, the stego image does not altered and the quality is retained, where as the extracted images do not have good quality for the that only one bits of LSB are utilized and it does adapt all the bits of the message image, resulting in the distortion during extraction. When we increase the no of bits to 2 bits of LSB, the PSNR value improves to 36.9851 and the MSE value 4.7908. Compared to 1 bit inversion, 2 bit inversion has an improved image quality in both stego image and extracted image. When we increase the bit inversion to 3 bits, the PSNR value gets improved to 39.6532 and the MSE 4.3815, at 3 bits inversion the extracted message image quality considerably improves, while further increasing the bits to 4 bits, the message image quality is improved comparatively to 3 bits with PSNR value 42.5978 and MSE value of 3.5752 respectively. It is noted that the error rate for 3 bits inversion is higher than the 4 bits inversion, this difference in MSE values differs from image to image and depends on the intensity of the available most significant bits in the message image. Throughout our experiments, the message image size and cover image size are maintained to hold equal pixels, if the message image pixels has an increased pixels, the LSB in the cover image does have pixels to accommodate and the message image quality gets distorted.

The PSNR value and MSE value is calculated for elephant.png image and is given in table 4.2

Table 4.2 PSNR and MSE value of Elephant.png

Image	1 bit	2 bits	3 bits	4 bits
PSNR	33.2301	35.6741	38.8670	42.651
MSE	5.181	4.2243	3.9861	3.5317

We take bird.png image as cover image which is 256x256 pixel and land.png as message image which is also 256x256 pixel. We apply LSB bit inversion technique developed in Matlab. The PSNR value calculated for bird1.png and message image elephant.png with LSB of 1 is 11.019, the MSE is 5.181. For LSB 2 the PSNR value is 17.072 and MSE is 1.286, for LSB 3 the PSNR value is 23.083 and MSE is 322.243 and finally for LSB of 4 the PSNR value is 29.295 and MSE value is 77.083. If is found that the PSNR value starts to rise with increasing bit levels from 1to 4 and the MSE on the other had also increase and drops at LSB 4. The quality of the image improves slowly from Lower LSB to Higher LSB bits, i.e. From 1 to 4, at LSB 4 the quality of image is higher when compared to LSB 1.

IV.CONCLUSION AND FUTURE WORK

Image steganography is a method which is utilized to conceal secret content within an image. The binary bits of secret information are concealed in the binary of image and this marginally impacts the magnitude of color and brightness which is difficult to detect for a human eye. Several algorithms are used for image steganography, where some of them are complex and some of them are simple. In general images are the mostly used for steganography when compared to text, audio and video objects. Regarding digital images many dissimilar variety of formats are available and are used accordingly for particular applications. A simple image steganographic framework comprises an original image, called cover (I) image in which secret message image (M) is hidden or embedded along with a stego key (K), the stego key applied to conceal the data as well as to draw out. The purpose of using stego key is to allow for protection.

The proposed Bit inversion technique utilizes 3 and 4 bits on 8 bit images and allows retaining the image quality. It is found that proposed Bit inversion technique has higher performance rate with regards to retaining image quality of the stego image from the original image. The quality of the images is interpreted using PSNR and MSE values obtained. From the experiments conducted, the PSNR value starts to increase from 1 LSB to LSB 4, the image quality of the stego image was low at LSB 1 but stabilizes with increasing LSBits, at LSB 4, the quality of the image is highly improved and it is almost similar to the original image. From the security point of view, at LSB 3 and 4 bits provide enhanced security for the message image and no one can easily find the combinations of 3 bits and 4 bits respectively. In future work, other bit combinations of cover image pixels can be considered. Leaving the LSB there are 21 (7C2) bit combinations of two bits in a pixel. We can also consider more bits of cover image pixels for analysis.

V. REFERENCES

[1]. Mork el, T., Eloff, J. H. P. and Oliver, M. S.; "An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA), 2005.

[2]. Zhang, T., Li, W., Zhang,Y. and Ping, X. ;" Detection of LSB Matching Steganography Based on Distribution of Pixel Difference in Natural Images", International Conference on Image Analysis and Signal Processing (IASP), pp.629-632, 2010.

[3]. Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.

[4]. Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998

[5]. Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[6]. Stefan Katzenbeiser & Fabien A.P.Petitcolas(1999), Information HidingTechniques for Steganography and Digital Watermarking, Artech House, Computer Security series, Boston, London.

[7]. Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996.

[8]. M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I. Shamsuddin "Information Hiding using Steganography" 4* National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia. 2003 IEEE.

[9]. Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[10]. Niels Provos and Peter Honeyman, "Detecting Steganographic Content on the Internet," August 2001. [NDSS '02, San Diego (February 2002)]

[11]. Neil R. Bennett, JPEG STEGANALYSIS & TCP/IP STEGANOGRAPHY, University of Rhode Island , 2009.

[12]. F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, "Information Hiding – A Survey", in proceeding of IEEE, pp. 1062-1078, July 1999

[13]. A. Mishra, A. Gupta, and D. K. Vishwakarma, "Proposal of a new steganography approach", in Proceedings of International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009, pp.175-178.

[14]. M. A. B. Younes, and A. Jantan, "A new steganography approach for image encryption exchange by using least significant bit insertion", International Journal of Computer Science and Network Security, vol.8, no.6, pp.247-254, 2008.

[15]. H. J. Zhang, and H. J. Tang, "A novel image steganography algorithm against statistical analysis", in Proceedings of Sixth International Conference on Machine Learning and Cybernetics, 2007, pp.3884-3888.

[16]. H. Mathkour, G. M. R. Assassa, A. A. Muharib, and I. Kiady, "A novel approach for hiding messages in images", in Proceedings of International Conference on Signal Acquisition and Processing, 2009, pp.89-93

[17]. Furuta, T,.Noda, H., Niimi, M., Kawaguchi E,"Bit-plane decomposition steganography using wavelet compressed video", Joint Conference of the Fourth International Conference, 2(5): 970 - 974, 2003.

[18]. V.Karthekayani and kammalakan, "Conversion grayscale image to color image with and without texture synthesis", International journal of computer science and network security, 7(4):11-16, 2007.

[19]. Brisbane, G., Safavi-Naini, R.&Ogunbona, P. (2005). High-capacity steganography using a shared colour palette. Vision, Image and Signal Processing, IEE Proceedings, 152 (6), 787-792.

[20]. Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm" Jordan Journal of Science publications, 3 (4): 223-232,2007.

[21]. Mamta Juneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.

[22]. P.Thiyagarajan, V.Natarajan, G.Aghila, V.Pranna Venkatesan, R.Anitha, (2013) "Pattern Based 3D Image Steganography", 3D Research center, Kwangwoon University and Springer 2013, 3DR Express., pp.1-8.

[23]. Shamim Ahmed Laskar and Kattamanchi Hemachandran, (2013) "Steganography Based OnRandom Pixel Selection For Efficient Data Hiding", International Journal of Computer Engineering and Technology, Vol.4, Issue 2, pp.31-44.

[24]. M. Juneja, and P.S. Sandhu, "Designing of robust image steganography technique based on LSB insertion and encryption", in Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp.302-305.

[25]. S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain", International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp. 2632-2637.

[26]. G. Swain, and S. K. Lenka, "LSB array based image steganography technique by exploring the four least significant bits", CCIS vol 270, part II, 2012, pp.479-488.

[27]. G. Swain, D. R. Kumar, A. Pradhan, and S. K. Lenka, "A technique for secure communication using message dependent steganography", International Journal of Computer and Communication Technology, vol.2, no. 2- 4, pp.177-181, 2010.