International Journal of Computer Applications Technology and Research
Volume 5–Issue 10, 678-682, 2016, ISSN:-2319–8656

Enhancement of Payload Capacity for Image Steganography based on LSB

Vidya Verma
Guru Jambheshwar University of Science and Technology,
Department of Computer Science and Engineering, Hisar, Haryana, India

Abhishek Kajal
Guru Jambheshwar University of Science and Technology,
Department of Computer Science and Engineering, Hisar, Haryana, India

Isha Kajal
Indus institute of Engineering and Technology,
Department of Computer Science and Engineering, Rohtak Road, Jind, Haryana, India

Abstract: In this result paper we will show the implementation result of our proposed method. Steganography is an art and science of Hide the data in a cover image using some techniques that it remains undetected by the unauthorized access. We hide the data in a manner that the stego image looks like a single entry by any third person. No one has doubt that the image is the stego image. We use some different methods that keep data to be secret. It is a powerful tool for security with which we can keep the data secret behind an object. An object may be Text, Audio, Video, and Image. The factor that affects the steganography methods are PSNR, MSE, Payload Capacity and BER. Security of data will be shown by the Histogram of picture.

Keywords: Steganography, PSNR, MSE, Stego-Image, Stego-Key, Data covering, Data Extraction.

1. INTRODUCTION TO STEGANOGRAPHY

Exponentially increase in the use of internet it becomes important to secure the confidential data and information on internet. Therefore, to cover the defensive information on the internet various. To avoid these problems many methods are used to hide the data in digital media

One is Cryptography, it only keeps the contents of the message secret i.e. No one can understands the secret message. But sometimes it is necessary to keep the existence of the message is secure that no one can think even a single secret bit is existing. So, a technique which keeps the existence of a message secret is known a steganography [1].
Steganography is a Greek origin word that means **"HIDDEN WRITING"** Steganography is an art and science of hiding information [2] in some cover media. It aims is to hide the presence of the secret message behind any object (Text, Image, Video, Audio) file By embedding one piece of data inside of another, the two entity become a new single entity, thus eliminating the need to keep a link between the two
distinct pieces of data, or risk the chance of their separation. After hide the message in any object file –called Stego Image. In this technology we will use many type of techniques using different type of the cover objects.

One application that demonstrate the advantage of this regards of steganography is the embedding of patient information within the medical imaging. By doing so a persistent association between these two information objects is generate [3]-[5].

"What You See Is What You Get" this concepts which we encounter sometimes does not always hold true. Images can be more than what we see with our Visual System; hence they can convey more than merely 1000 words. Figure1.1 (Types of the Steganography cover objects) shows how a Stenographic system works [6]-[7].

1.1 Motivation

Exponentially increase in the use of internet it becomes important to secure the confidential data and information on internet. Hence, there is need to cover the defensive information on the internet. Those days are gone when we use the image for our memorable part, Audio as our favourite songs, Video as our favourite movie or song. In the digital world we use image, audio, video as our containers. In earlier, the use of the internet is increasing exponentially. So the unauthorized access of the data is also increase day by day. So we need some secure method preventing from this type of access. We can secure our data using cryptography and steganography. Cryptography is a technique which can encrypt the data in an another form called cipher text using a key(Symmetric & Asymmetric key).If the third party knows the key of the cipher text then he can access the data. But if we hide the existence of the data. Then the third party don't know about the existence of the data. So data is secured from the unauthorized access. This is called steganography. So it is a motivational point that time we need it.
To hide the secret data we need some terminology:

- Secret data that must be hidden (M); it may be plain text or may be Cipher text.
- Cover object (C) that works as a container in which we will hide the data.
- Stego encoding (Se) and decoding(Se^{-1})
- A stego key (K) which is used at the time of encoding and at the time of decoding.
- A Payload capacity is a capacity that a Cover Object can contains the secret bits.

The main terminology in the steganography is the objects that we use to hide the data called cover objects. There are many types of the cover objects we have. Cover object is the object which is used to hide the secret bits in the bits of the cover objects bits. We have to modify the bits to hide the data in the cover objects. We can use the audio, video, image, text, any type of puzzles and network protocol (PDU). Behind these objects we can hide the data which we want to hide. Using the techniques of the data hiding we can hide the data.

In the steganography process before hiding the data we must chose the object that was used in the data hiding. It may be text Image audio and video. Then enter the data that will be hidden and apply some technique on the secret data to make it more secure. We can encode it or also encoding with compressing the data. It will provide more security than the normal data. After encoding the data we will secure it by a security key that is known by only receiver. And then apply the steganography technique on it. After it sends to the receiver .Receiver performs the reverse process of steganography with the help of the Security key and extract all the information. The Process of steganography is shown in figure 1.1.

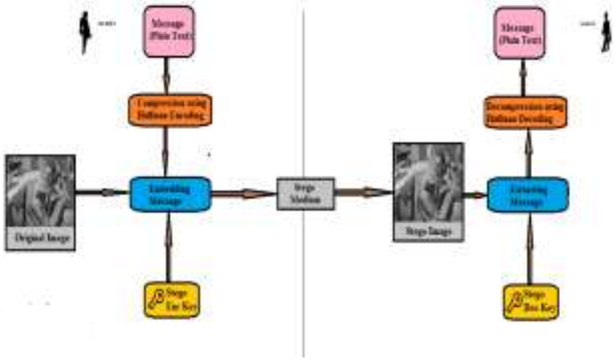


Figure 1.1 Process of embedding the data and extracting the data.

Least significant bit technique is mainly used or we can say that generally used because it is so easy to implement and also steganalysis is easy in it .So to find the data in this approach is very easy so to secure the data we can use different technique to improved it.

We can apply the techniques to make it more secure. Image steganography is used mainly to send the data because everyone not known to this technology so he or she treat an image as an image. There are two types of images are grey scale image and true color image .In the grey scale image a pixel value is 8 bit but in true color image a pixel value is 24 bits.8 bit for red color, 8 bit for green color and 8 bits are for blue color. When e grey scale image is used for LSB the generally the least significant bit is modified or only one bit is modified but in the true color image a pixel have 24 bits so there are 3 bits to modify. This LSB method is using because it is easy and also enhance the quality of image. There is high SSIM index in this technique.

In this paper we proposed a more efficient LSB technique with more Security and more data saving in the image. And also used a security key to prevent from the unauthorised access. In the implementations results shows that after proposed method a picture can contain more data than the previous one and less distortion in the image and less bit error rate. The starting of hiding the data is not from the initials but form 2nd Row and 2nd columns .So no one can knows that from where insertion or replacing the bit is on initially.

2. RELATED WORK

LSB is simplest method to be implemented with any type of image either JPEG or BMP. It will work with the grey type image or also true color image. In true color image there are 24 bits in which 3 bits are replaced by the secret data. And in grey scale image one bit is replaced as shown in the example. These are the 3 pixels with red green blue pixel values. Now according to LSB the least significant bit is replaced by the secret message bits that already converted into ASCII code.

Before applying LSB

11001011	00101111	01011100
00110011	10001010	10000110
11001110	01101111	11000100

Now let the data that will be hidden is 101011010 in the pixel values of true color image. Replacing the LSB bit by the secret bits. And the result is as follows:

After applying LSB

11001011	00101111	01011100
00110011	10001010	10000111
11001110	01101110	11000101

So according to this process we can say that

Stego Image =Cover image + Secret Data at the time of embedding the data in the cover image but at the time of extraction of the data is:

Secret data + Cover image = Stego image.

Some of the measure are here that affects the steganography. These measure shows how reliable or good is our steganography. These are PSNR, BER, and SNR Of the image.

PSNR is peak signal to noise ratio that shows ratio between the maximum possible power of a signal and the power of corrupting noise that reflects the accuracy of its representation as in (1).

$$\text{PSNR}= 10*\log10\ (Q*Q/\text{MSE}) \tag{1}$$

Q is 255 in the case of grey scale image.

The Bit error rate is defined that the reciprocal of Peak signal to noise ratio as (2). Smaller the BER Higher the Quality.

$$\text{BER}=1/\text{PSNR} \tag{2}$$

MSE (Mean Square Error): It is described as metrics of error used to compare image compression as in (3). The mean square error represents the progressive average squared error difference between an original picture and the changed image.

$$\text{MSE} = \text{sum}\ (\text{sum}\ (\text{img\_def}.\ \hat{}2))/\text{nRow} / \text{nColumn} \tag{3}$$

3. PROPOSED METHOD

The Proposed work include the data hiding with the compression of the data that to be hidden. We hide the data from specified pixel that it may difficult in steganalysis.

Method used in the dissertation hides the data in specific bit position combinations of LSBs instead of hiding the data only in least significant one bit. In our proposed system we will concentrate on the maximization of the payload capacity with less degradation in the image. We also used the reduction (Huffman coding) on the secret bits so we can more data hide in the cover object. It not just provide data reduction also provide encryption or data encoding because after implementing of Huffman coding it gives output in reduction and in encoded form. So it is an advantageous for us that data is also encoding so the time factor is also less in it for data extraction. It also provide security in manner that how it will encode (Huffman code) the confidential data. It provides two level of security.

In this to find the specific bit position we use 3^n where n<=1.There is a reason for that because a pixel is of 8bit if grey scale image or 24 if true color image. When grey scale image then 8 bits are here for LSB insertion then to find the bit position n=1 not greater than 3 because 3^1=3 and 8 bits are there or in case of true color image R(red),G(green),B(blue) are used and a pixel use 8 bit for each then 24 bits are used. And LSB insertion is for each R, G, and B.

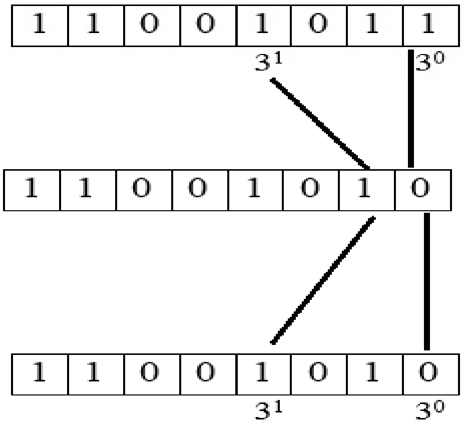
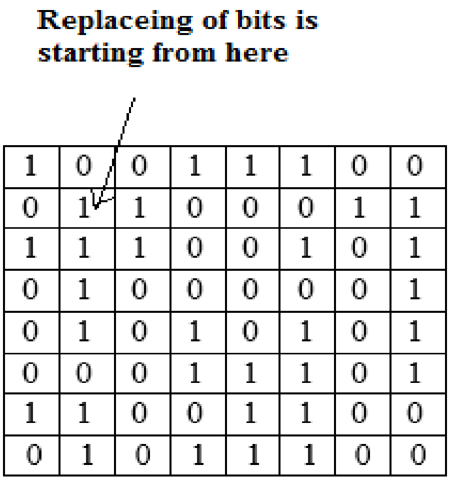


Figure 1.3 Proposed method

It is more efficient than all LSB insertion techniques. The extraction of the message is reverse process that finds the bit position and the collect the confidential data bits. While extracting the secret data then it is lossless data extraction mean no information loss at the time of the data extraction.



1	0	0	1	1	1	0	0
0	1	1	0	0	0	1	1
1	1	1	0	0	1	0	1
0	1	0	0	0	0	0	1
0	1	0	1	0	1	0	1
0	0	0	1	1	1	0	1
1	1	0	0	1	1	0	0
0	1	0	1	1	1	0	0

Figure 1.2.2 starting of replacing the encoded bit

ALGORITHMS: The Proposed hiding Algorithm
INPUT: TRUE COLOR IMAGE, SECRET MESSAGE, SECURITY KEY
OUTPUT: STEGO IMAGE

START

1. SCAN THE IMAGE ROW BY ROW AND CONVERT IT IN THE PIXELS SEPARTE VALUE IN RGB OR IN BINERY VALUES.
2. TAKE THE SECRET DATA AND COVERT IT ITS CORRESSPONDING ASCII CODE.
3. NOW COMPRESS THE CODES WITH THE HUFFMAN CODING, IT ENCODEING THE MESSAGE ALSO REDUCE THE MESSAGE.
4. CHECK THE SIZE OF IMAGE AND ALSO THE SECRET MESSAGE

    - CHOOSE PIXEL H=WHERE WE START TO HIDE THE DATA SHOWN IN FIGURE 1.3.
    - DIVIDE THAT PIXEL INTO 3 PART RED, GREEN, BLUE.
    - HIDE THE COMPRESSED DATA IN POWER 3 BIT PLACE IN THE VALUES OF PIXEL.
    - IF BITS ARE SAME THEN REPAEAT OTHERWISE REPLACE THE BIT IN IMAGE.
    - SAVE THE LOCATION OF HIDING THE BIT
    - ENTER THE SECURITY KEY KNOWN BY ONLY RECIEVER,

5. SET THE NEW VALUES OF IMAGE AND SAVE IT.

END

4. EXPERIMENT RESULT

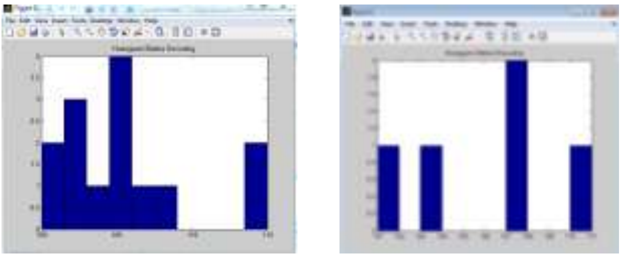
Experiment result section is used to show the implemented results of the proposed method. The result will be shown in of the form graphs and tables. We take some standard picture to show the results named as Lena, peng and joshi as cover image used to hide the message in it. Some data is entered to hide.

(Joshi)

(Lena)

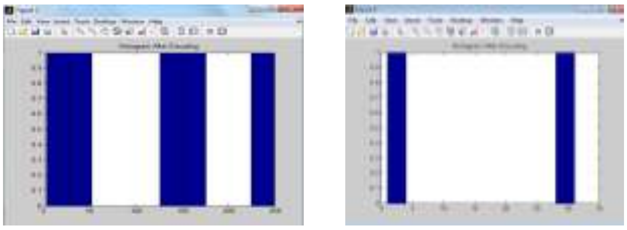
(Peng)
Figure 1.4 Original Cover image

The Procedure of hiding data is shown in figure 1.2. It shows the whole process of our proposed work. Various performance parameters like PSNR, MSE, BER, payload capacity, Histogram for security and compression ratio is also used to fine out the compressing bit. These are used to evaluate the performance of the purpose method. The performance is taken out from various images and embedding data in the ASCII Format. Figure no 5.1 to figure no 5.22 shows the different phase with factors that affecting our steganography and Table no 2 shows the result of the three images.



(joshi.jpeg) (Lena.jpeg)

Figure 1.4 Histogram before Steganography



(joshi) (Lena)
Figure 1.5 Histogram of after Steganography.

Figure 1.4 and 1.5 shows the histogram of the data before and after the steganography. Histogram is used to show the security of our data that how much it is secured.

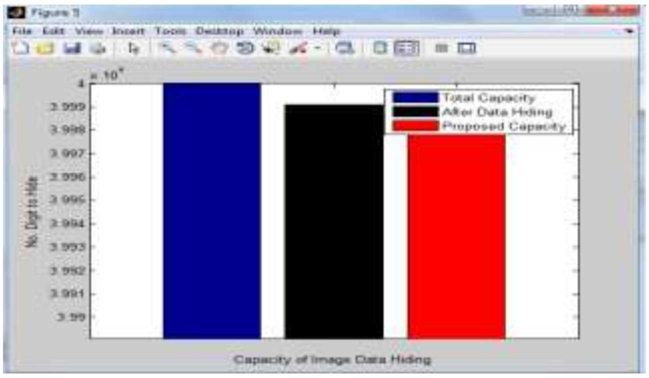


Figure 1.6(joshi) Graph shows the capacity ratio of image

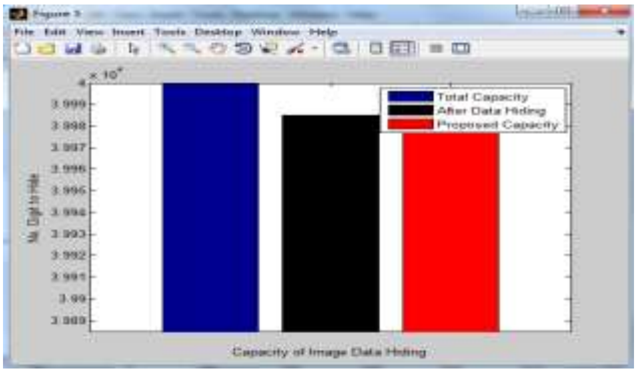


Figure 1.7(Lena) Graph shows the capacity ratio of image

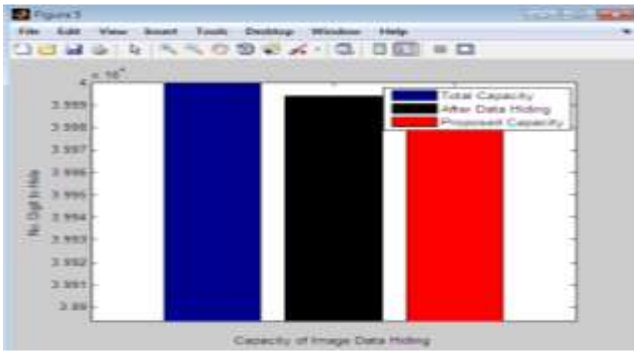


Figure 1.8(Peng) Graph shows the capacity ratio of image

Figure 1.6, 1.7, and 1.8 shows the comparison between maximum capacity, uncompressed and proposed system. This graphs shows that proposed system shows the high capacity than uncompressed data. So we will able to maximize the size using this system. Other results are shown through the table.

Table 1 Results and Observation

Cover Image	Before Compression	After Compression	PSNR	BER	MSE
	39985	39995	88.8920	0.01243	0.5250
	39983	39993	91.4054	0.02123	0.3062
	39988	39995	87.6426	0.01989	0.21250

5. CONCLUSION

Table 1 shows the results and observations of the proposed system. Here are the results of the system in the tabular form. This observation shows that the proposed system is better from the previous technique. The Parameters used to define the proposed system is better than the previous one technique are Payload capacity, PSNR, BER, MSE. The parameter are used to compare the results define less error rate and noise ratio. And less degradation in the image quality after the proposed system. The main aim of my dissertation is to enhance the payload capacity and we meet our aim in the dissertation. Less visible to human eyes and results are meets to our objectives of our dissertation.

6. REFERENCES

[1] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. “An overview of image steganography." In ISSA, pp. 1-11. 2005.

[2] Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn. "Information hiding-a survey." Proceedings of the IEEE 87, no. 7, 1062-1078, 1999.

[3] Marvel, Lisa M. "Image steganography for hidden communication." PhD diss., University of Delaware, 1999.

[4] Chandramouli, Rajarathnam, Mehdi Kharrazi, and Nasir Memon. "Image steganography and steganalysis: Concepts and practice." In International Workshop on Digital Watermarking, pp. 35-49. Springer Berlin Heidelberg, 2003.

[5] Al-Mohammad, Adel. "Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility." PhD diss., Brunel University, School of Information Systems, Computing and Mathematics Theses, 2010.

[6] Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." In ISSA, pp. 1-11. 2005.

[7] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." Signal processing 90, no. 3 727-752, 2010.

[8] Vaishali and Abhishek Kajal, “Increasing Data Hiding Capacity of Carrier Image Using BPCS Steganography”, International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Volume 4, Issue 5, May 2015, PP 434-437.

[9] Vidya , Abhishek Kajal, “A Short Survey on Cover Objects for Hidden Communications”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 5, May 2016.