Mr. Gaurav al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 2, Issue 4, December 2015, pp. 169-174

A New Method for Image Steganography Using LSB and MSB

Mr. Gaurav

Assistant Professor, Department of CSE, FET, Jamia Hamdard University, New Delhi - 62, India

Abstract: **Image steganography is the art of hiding information. In this technique data is embedded into an image. Bits of information are placed in pixel values of image so that attacker cannot find out where data is hidden. In this paper a new information hiding method is proposed. In this method we have used the concept of spatial domain for hiding and retrieval of the information i.e. the use of pixel values. In this paper we have used the LSB and MSB pixels for hiding and retrieval of the message. Also the advantages and disadvantages of the proposed method have been discussed.**

Keywords: **LSB, Data hiding, steganography, PSNR, MSE**

I. INTRODUCTION

With the growth of computer network, security of data has become a major concern and thus data hiding technique has attracted people around the globe. Steganography techniques are used to address digital copyrights management, protect information, and conceal secrets [1]. Data hiding techniques provide an interesting challenge for digital forensic investigators. Data is the backbone of today's communication. To ensure that data is secured and does not go to unintended destination, the concept of data hiding came up to protect a piece of information. Digital data can be delivered over computer networks with little errors and often without interference. The Internet provides a communication method to distribute information to the masses. Therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. Steganography and cryptography are two different information hiding techniques, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Steganography relies on hiding message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. The technique replaces unused or insignificant bits of the digital media with the secret data. The concept is to embed the hidden object into a significantly larger object so that the change is undetectable by the human eye. All digital file formats can be used for steganography, but the formats those are with a high degree of redundancy are more suitable. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. The most popular cover objects used for steganography are digital images. Digital images often have a large amount of redundant data, and this is what steganography uses to hide the message. Cryptography merely obscures the integrity of the information so that it does not make sense to anyone except the creator and the recipient. Steganography could be considered as the dark cousin of cryptography. Cryptography assures privacy whereas Steganography assures secrecy [2]. Steganography and cryptography are both used to ensure data confidentiality. However, steganography differs from cryptography in the sense that the cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Thus, with cryptography anybody can see that both parties are communicating in secret. Steganography hides the existence of a secret message in such a way that nobody can see that both parties are communicating in secret.

The basics of embedding data rely on three different facts i.e. capacity, security, and robustness.

Capacity means the media on which the data is to be hidden should hold the data, so that the complexity of the medium should not be disturbed [7]. Security means the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks [8]. Finally, robustness means the amount of manipulation a cover image (original image) can handle without drawing any attention that a change has taken place. Steganography and cryptography have to guarantee any of the requirements. Steganography and Cryptography are parallel data security techniques and the techniques can be implemented side by side, in fact steganographic system can implement cryptographic data security. With cryptography we can protect the message but not hide its existence. Steganography pay attention to the degree of invisibility while cryptography pays attention to the security of the message. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be increased by combining it with cryptography.

II. PROPOSED METHOD:

In this method, first and last bits of image are extracted from pixels values of an image. The possible combination of these two bits are 00, 01, 10 and11. If we want to embed 0 and the combination are 00 and 11 then 0 is embedded but if the combination are 01 and 10 then they are made 00 or 11 by adding or subtracting 1 from the least significant bit. If the

data bit is 1 and the combinations are 01 and 10 then the data bit is embedded otherwise if the combinations are 00 and 11 then they are made 01 and 10 by adding or subtracting 1 from the lsb. At the time of retrieval if the combinations come out to be 00 and 11 then the data bit is taken as 0 otherwise it is taken as 1. The algorithm for our method is given below:

Step1: Import image using imread() function.

Step2: Select image and convert into gray scale using formula rgb2gray(RGB) using the following formula:

j=0.2990*R(i)+0.5870*G(i)+0.1140*B(i)

Step 4: Embed encrypted text into image.

Step 5: Decrypt text from image.

Step 6: Retrieve the text.

FLOWCHART OF THE PROPOSED METHOD

The flowcharts for insertion and retrieval of message bits using the proposed technique are given below which describes the process briefly:

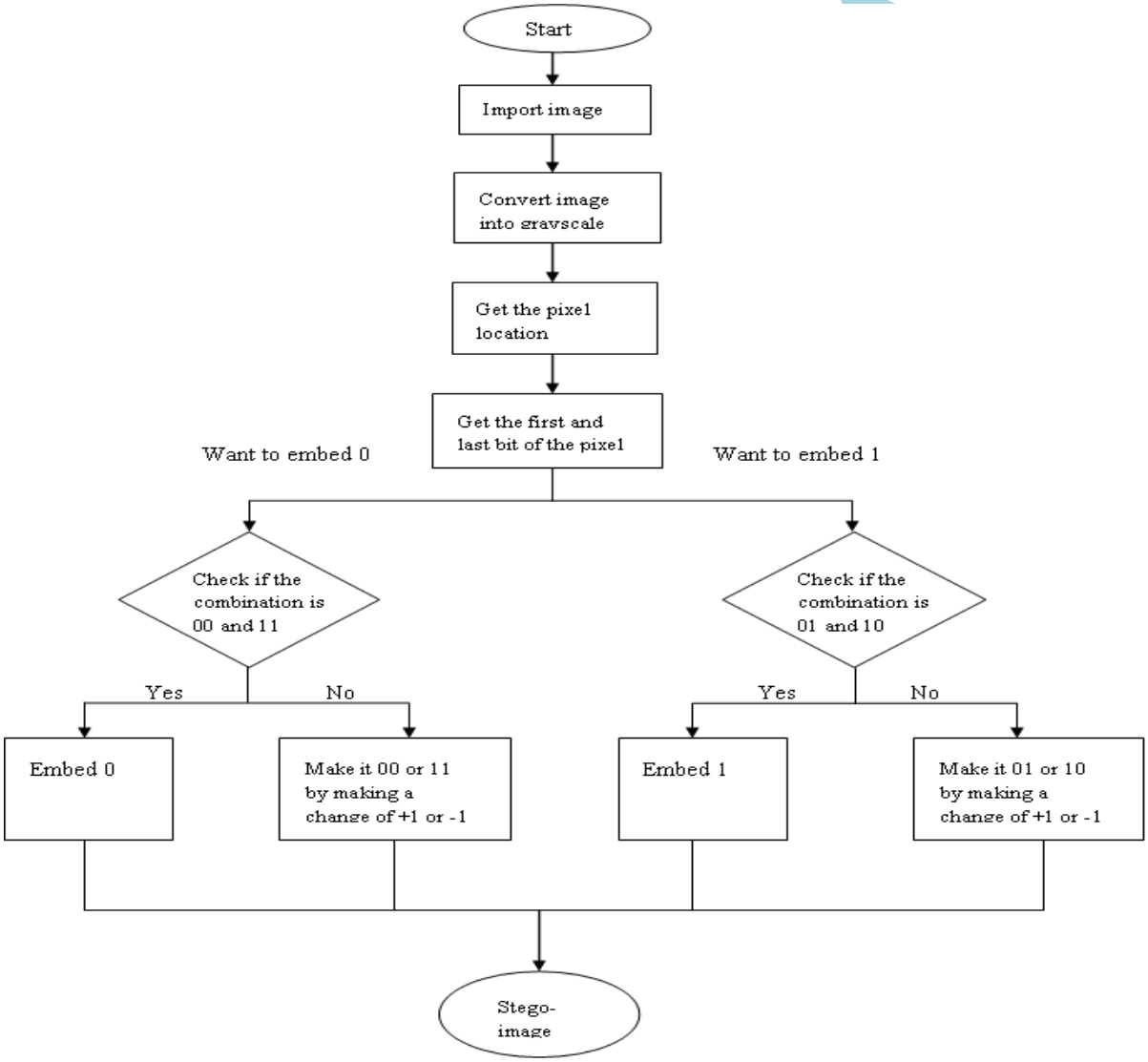

Figure 1: Flowchart depicting insertion of message bits

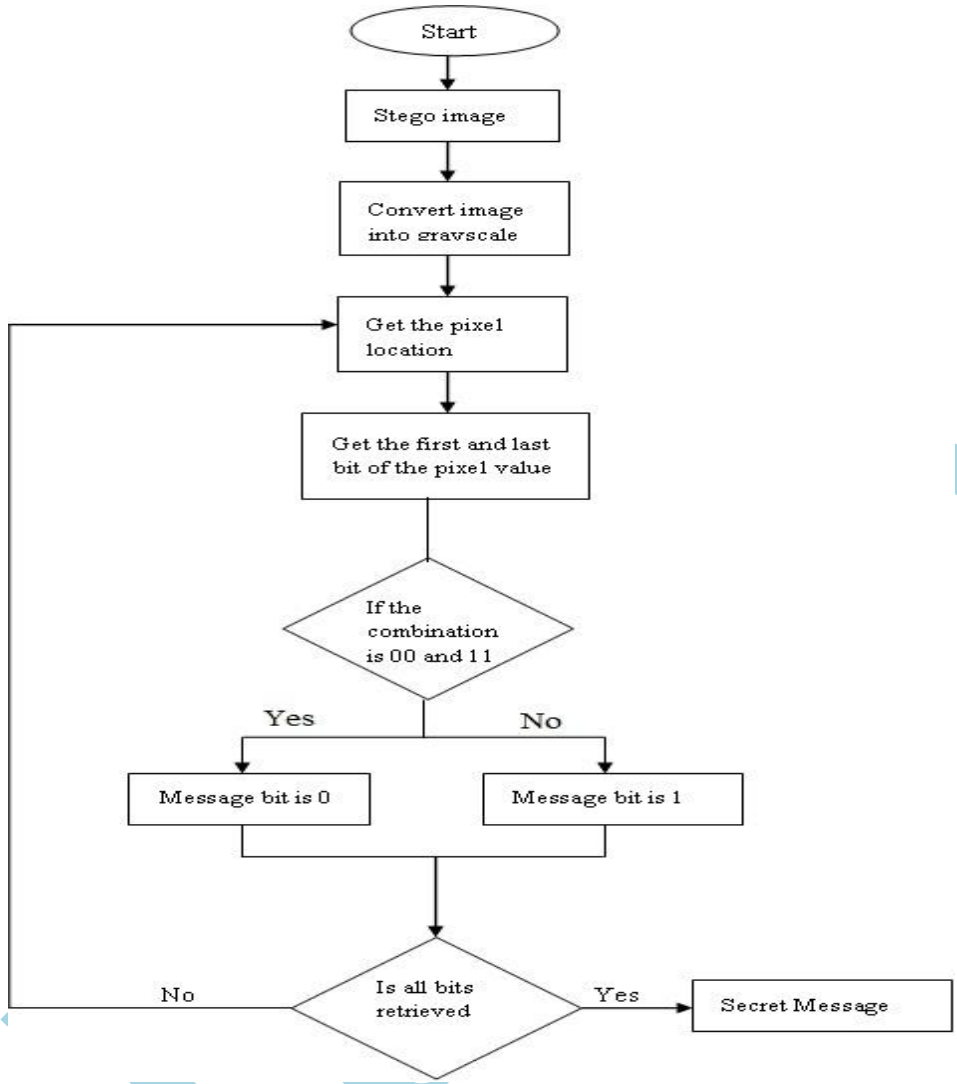

Figure 2: Flowchart depicting retrieval of message bits

ALGORITHM FOR INSERTION OF MESSAGE

(i) Find the pixel location (L) in cover image from secret key to insert the message bit.

(ii) If we want to insert 0 then go to step (iii) else go to step (iv).

(iii) (a) If bits are 00 or 11 then insert then no change is required message bit is already there.

(b) If bits are 01 and10 make them 00 or 11 by adding or subtracting 1.

(iv) (a) If bits are 01 or 10 then no change in message bits.

(b) If bits are 00 and11 make them 01 or 10 by adding or subtracting 1. (i)

(v) END

ALGORITHM FOR RETRIEVAL OF MESSAGE:

(i) Trace out the location (L) from the same secret key as used for insertion of message.

(ii) Check at location (L):

(a) If first and last bits are 00 or 11 then message bit is 0.

(b) If first and last bits are 01 or 10 then message bit is 1

(iii) END

III. RESULTS AND CONCLUSION

The following results obtained from Table 1 and Table 2 tells us how our method is better than previous methods.
The message bit will be inserted at the pseudo random location at first chance

= 512/512*100= 100%

(ii) Chance when message is inserted, no change in pixel value is required

= 258/512*100= 50.39%

Table 1: Change in pixel value after insertion of '0'

Decimal value	Pixel value before insertion	Pixel value after insertion	Change in Pixel Value & Comment
0	00000000	00000000	NC, Insert
1	00000001	00000000	-1 insert
2	00000010	00000010	NC ,Insert
3	00000011	00000010	-1,insert
4	00000100	00000100	NC, Insert
5	00000101	00000100	-1,insert
6	00000110	00000110	NC, Insert
7	00000111	00000110	-1,insert
8	00001000	00001000	NC, Insert
9	00001001	00001000	-1,insert
10	00001010	00001010	NC, Insert
11	00001011	00001010	-1,insert
12	00001100	00001100	NC, Insert
13	00001101	000011010	-1,insert
14	00001110	00001110	NC, Insert
15	00001111	000011110	-1,insert
-			
-			
-			
127	01111111	01111110	-1,insert
128	10000000	10000001	+1,insert
-			
-			
254	11111110	11111111	+1,insert
255	111111111	111111111	NC, Insert

Table 2: Change in pixel value after insertion of '1'

Decimal value	Pixel value before insertion	Pixel value after insertion	Change in Pixel Value & Comment
0	00000000	00000000	+1, insert
1	00000001	00000001	NC, insert
2	00000010	00000011	+1 ,Insert
3	00000011	00000011	NC, insert
4	00000100	00000101	+1 ,Insert
5	00000101	00000101	NC, insert
6	00000110	00000111	+1 ,Insert
7	00000111	00000111	NC, insert
8	00001000	00001001	+1 ,Insert
9	00001001	00001001	NC, insert
10	00001010	00001011	+1 ,Insert
11	00001011	00001011	NC, insert
12	00001100	00001101	+1 ,Insert
13	00001101	00001101	NC, insert
14	00001110	00001111	+1 ,Insert
15	00001111	00001111	NC, insert
-			
-			
-			
127	01111111	01111111	NC, insert
128	10000000	10000000	NC, insert
-			
-			
254	11111110	11111111	NC, insert
255	11111111	11111110	+1, Insert

NC = No Change

In given fig 3 and 4 shows the cover image Lenna with its stego image. The PSNR and MSE values have been shown between original Lenna cover image and Lenna stego image and their histogram also shown in figures 5 and 6

Fig 3

Fig 4

PSNR between Image (1) and Image (2) = +42.01

MSE between Image (1) and Image (2) = 0.0071

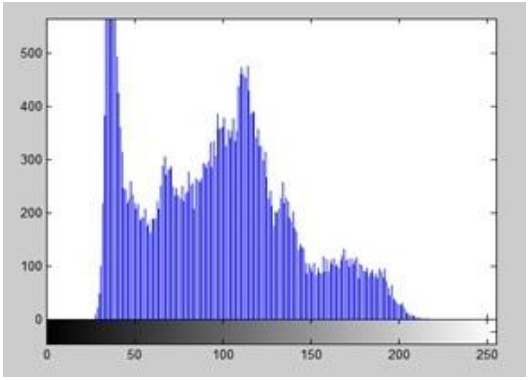

Fig.5 Histogram of Original Image

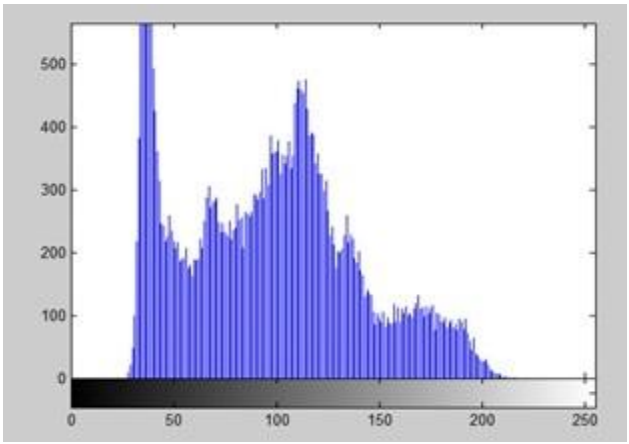

Fig 6: Histogram of Stego Image

Fig.7 and 8 shows the cover image Baboon with its stego image. The PSNR and MSE values have been shown between original Baboon cover image and stego Baboon image and their histogram also shown in figures 9 and 10.

Fig 7

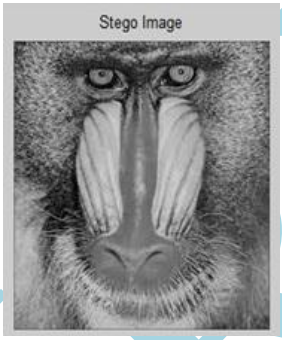

Fig 8

PSNR between Image (1) and Image (2) = +46.04

MSE between Image (1) and Image (2) = 0.0044

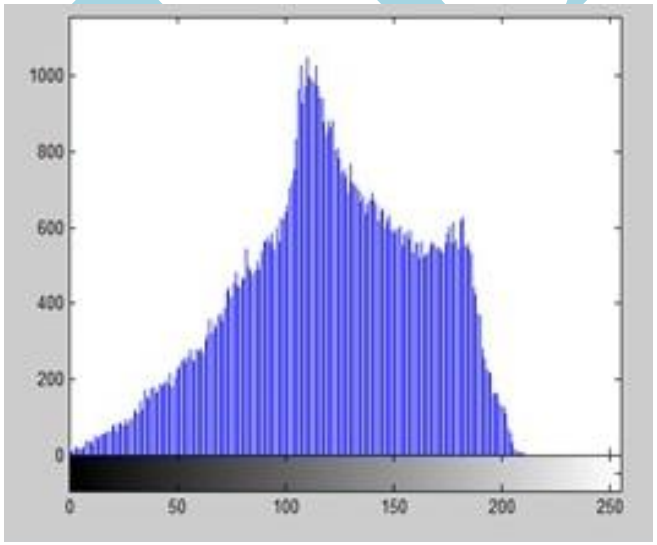

Fig 9: Histogram of Original Image

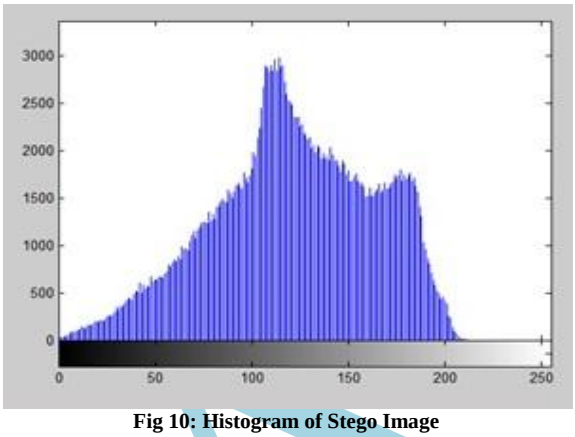

Fig 10: Histogram of Stego Image

From the above discussion, we can say that our method is better than the other methods for the following reasons:

(a) It provides 100% for message insertion.

(b) Change in image required is less than previous methods.

IV. REFERENCES

[1] Anderson , R. J. and Petitcolas, F. A.P. (1998) "On The Limits of Steganography", *IEEE Journal of Selected Areas in Communications*, Vol.16 No.4, pp.474-481, ISSN 0733-8716.

[2] Petitcolas, F.A.P., Anderson, R. J. and Kuhn, M.G. (1999) "Information Hiding -A Survey", *Proceedings of the IEEE*, Special issue on Protection of Multimedia Content, vol. 87, no. 7, pp.1062- 1078.

[3] Neil F Johnson, Sushil Jajodia, "Exploring Steganograph: Seeing the Unseen", IEEE Computer, pp 26-34, Feb 1998.

[4] Vidyasagar M. Potdar, Elizabeth Chang, "Gray Level Modification Steganography for Secret Communication", 2nd IEEE International Conference on Industrial Informatics INDIN 2004 June 24th, 26th June, Berlin, Germany, Submitted Tuesday, May 25, 2004

[5] R., Chandramouli, and Nasir Memon.(2001), "Analysis of LSB based image steganography techniques." In *Image Processing, 2001. Proceedings. 2001 International Conference on*, IEEE, vol. 3,pp. 1019-1022.

[6] Huang, Y. S., Huang, Y. P., Huang, K.N. and Young, M. S. (2005), "The Assessment System of Human Visual Spectral Sensitivity Curve by Frequency Modulated Light", *Proceedings of the*

2005 IEEE Engineering in Medicine and Biology 27th Annual Conference, pp. 263-265.

[7] Laskar, S.A. and Hemachandran, K. (2012), "An Analysis of Steganography and Steganalysis Techniques", *Assam University Journal of Sscience and Technology*, Vol.9, No.II, pp.83-103, ISSN: 0975-2773.

[8] Dunbar, B. (2002). "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment", *SANS Institute 2002*, pp.1-9, http://www.sans.org.

[9] Kruus, P., Caroline, S., Michael, H. and Mathew, M. (2002), "A Survey of Steganographic Techniques for Image Files", *Advanced Security Research Journal, Network Associates Laboratories*, pp.41-51.

[10] Kharrazi, M., Sencar, H. T. and Memon, N. (2004), "Image Steganography: Concepts and Practice", *WSPC/Lecture Notes Series: 9in x 6in*, pp.1- 31.

[11] Chandramouli, R. and Menon, N. (2001), "Analysis of LSB based image steganography techniques", I*EEE Proceedings on Image Processing*, Vol.3, pp.1019-1022.

[12] Tiwari, N. and Shandilya, M. (2010), "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", *International Journal of Computer Applications* (0975 – 8887) Vol. 6, no.2, pp.1-4.

[13] Deshpande, N., Kamalapur, S. and Daisy, J. (2006), "Implementation of LSB steganography and Its Evaluation for Various Bits", *1st International Conference on Digital Information Management*, pp.173-178.

[14] Celik, M. U., Sharma, G., Tekalp, A.M. and Saber, E. (2005), "Lossless Generalized-LSB Data Embedding", *IEEE Transaction on Image Processing*, Vol. 14, No. 2, pp. 253-266.

[15] Brisbane, G., Safavi-Naini, R. and Ogunbona, P. 2005. "High-capacity steganography using a shared colour palette", *IEEE Proceedings on Vision, Image and Signal Processing*, Vol.152, No.6, pp.787-792.

[16] Karen, Bailey, and Kevin Curran.(2006) "An evaluation of image based steganography methods" Multimedia Tools and Applications, Springer Vol.30, no. 1, pp. 55-88.

[17] Gutte, R. S. and Chincholkar, Y. D. (2012) "Comparison of Steganography at One LSB and Two LSB Positions", *International Journal of Computer Applications*, Vol.49,no.11, pp.1-7.

[18] Deshpande, N., Kamalapur, S. and Daisy, J. (2006), "Implementation of LSB steganography and Its Evaluation for Various Bits", *1st International Conference on Digital Information Management*, pp.173-178

[19] Chan, Chi-Kwong, and L. M. Cheng. (2004), "Hiding data in images by simple LSB substitution." *Pattern Recognition* Vol. 37, no. 3, pp. 469-474.

[20] Shamim Ahmed Laskar and Kattamanchi Hemachandran (2012) "High Capacity data hiding using LSB Steganography and Encryption" International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.

