# A Novel Approach for Data Hiding using LSB on Edges of a Gray Scale Cover Images

Krishna Nand Chaturvedi
Department of computer science and engineering
NITTTR, Chandigarh India
E 32 Sector9, New Vijay Nagar
Ghaziabad-201009

Amit Doeger
Department of computer science and engineering
NITTTR, Chandigarh India
Department of computer science and engineering
NITTTR, Chandigarh Sector 26
Chandigarh-160019

## ABSTRACT
At present, there are many data security mechanisms available in the information security horizon. Many of them mostly emphasize how to make an algorithm that is computationally hard decipher by a cryptanalysis attack. However, in day to day life computational power is increasing in the digital world. So recent trend in the data security paradigm is changing from one layer security to two-layer security first layer is called cryptography, which secured against cryptanalysis and second layer is steganography that prevents, as much as possible, against any suspicion of the hidden text. In this approach, firstly, it is required to extract all the three-color components of a digital image then to find the edges of each component. Since intensity values of edge pixels differ abruptly in comparison to nearest neighbor pixels, it will not arouse suspicion if the intensity values of these pixels are changed. Thus, embedding of the higher-order bits in the edge pixels is possible as compared to the lower-order bits in the non-edge pixels. Thus finally this work is more contributive towards the goal of increasing the embedding rate and strength against steganalysis attack in the edge based steganography.

## Keywords
LSB, EG-LSB, Data hiding, Steganography, Edge extraction, Canny Edge Detector etc…

## 1. INTRODUCTION
Throughout all eras, people sought techniques to exchange of information secretly. Out of many approaches, an earliest approach for doing this was the Wax Tablets used by the ancient Greeks. In 480BC, Demaratus had been used the Wax Tablets in an attempt to warn King Leonidas of Sparta that King Xerxes-I planned to win his army into Greece prior to the historic achievement of Thermopylae. Because the danger of being discovered was great, Demaratus hid his warning by scraping the wax off the tablets and scribing his message directly onto the wood. Then he re coated the tablets with wax and sent the tablets via messenger to Leonidas. Interestingly, when the tablets were delivered, no one could figure out why they had received wax tablets with nothing written on them. According to The Histories written by Herodotus, widely acclaimed as the Father of History, Queen Gorgo, Leonidas' wife is purported to have said, "If they scraped the wax off the tablet, they would be sure to find the writing upon the wood." Thus, the warning was delivered, but the Spartans got Mssacred at Theropylae in one of history's greatest last stands as depicted in the movie 300 starring Gerard Butler. A use of Wax Tablet by Demaratus was one of the earliest and most widely referenced uses of information hiding, a practice that has become known as steganography [24].Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message [2]. Due to growing need for security of data image steganography is gaining popularity [3].The main goal of steganography is to communicate securely in a completely undetectable manner [4] and to avoid drawing suspicion to the transmission of a hidden data. [5]-[7] discuss ancient steganography techniques. There are many steganography applications for digital image, including copyright protection, feature tagging, and secret communication [4, 8]. Unfortunately the members of terrorist organizations are using steganography as a tool to attack against the western interests [9]. In general, the information hiding process extracts redundant bits from cover object [10, 11]. The traditional image steganography algorithm is called Least Significant Bit embedding; the advantage of LSB is its simplicity to embed the bits of the message directly into the LSB plane of cover-image, and many applications use this method [12]. If a steganography method causes someone to suspect that there is secret information in the carrier medium, then this method fails [8]. The previous algorithms LSB concentrates on hiding data in the least significant bit position of all or some selected pixels thus they are not particularly concentrating on special pixels. Since edge pixels have lager differences in the values from their neighboring pixels [1]. To overcome these problems it is proposed a novel image steganography algorithm based on LSB embedding algorithm for hiding secret messages in the edges of the image.

The image steganography is the process in which we hide the data within an image so that there will not be any perceived visible change in the original image. The conventional image steganography algorithm is LSB embedding algorithm. Steganography can be applied to audio files, i.e., it can hide information in an audio file; it can be called Audio Steganography. The audio file should be undetectable. Steganography can be applied to video files, i.e., if there will hide information in a video file, it can be called Video Steganography. Steganography can be applied to text files, i.e., if there will hide information in a text file, it is called Text Steganography.

The general process of steganography i.e., preparing a stego object that will contain no change with that of original object is prepared but using text as a source. The basic image steganography algorithm is Least Significant Bit embedding. In a gray-scale image, each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by “1." So, this property is used to hide the data in the image. Here we have considered last two bits as LSB bits as they will affect the pixel value only by “3." This helps in storing extra data.

## 2. RELATED WORK

In this section, we review past work relevant to the problem of hiding text in an image file and then extracting the hidden message. The purpose of the literature survey presented here is describing earlier work done in the field of hiding the text and extracting text from a steganographic image. In each case, it summarizes the approaches and highlights the contributions, assumptions and limitations of each of these approaches. Zhe Wang [13] proposed to identify the LSB steganography in the digital signals such as images and audio. In that the length of hidden data is arrived at in such a manner that the original message can be recovered with high precision. The steganalysis approach that he proposed is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. To evaluate the robustness of the proposed steganalysis approach, bounds on estimation errors were developed. Andrew D. Ker [14] proposed to identify the spatial domain LSBM steganography in gray scale images, which proved to be much harder than for its counterpart, LSB replacement. The HCF, for the detection of steganography in color images but ineffective on gray scale images. Q. Huang [15] proposed the problem in LSBMR algorithm to make regions selection on images to find suitable area. By counting on each pixel we can decide whether it should be protected or not. It can improve the visual imperceptibility and detect ability of the LSB matching method. By adjusting the parameters of neighbor pixels, the max embedding capacity can be increased as needed. A.D. Ker [16] proposed the general framework for detection and length estimation of these hidden messages, which potentially makes use of all the combinatorial structure. It is necessary to screen the Triples method by first applying a standard estimator, because of inaccurate results when the hidden message length is high. A range of experiments verify that this makes for a reliable detector and estimator of hidden messages, performing somewhat better than the standard detectors on uncompressed covers, and very much better on images where the cover has artifacts. A. Almohammad [17] proposed the performance of both gray scale and color versions of a given cover image when they are used with a given steganography method, the capability and impact of using the chrominance components for data hiding. There are two steganography methods are used as test methods, JSteg and JMQT. As a result, using color images is better than using gray scale images for data hiding. Milelikainen [18] proposed the modification to the LSBM choice of whether to add or subtract one from the cover image pixel is random. The embedding is performed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. Therefore, the modified method allows embedding the same payload as LSB matching but with fewer changes to the cover image. Xinpeng Zhang [19] proposed a novel steganography scheme that employs human vision sensitivity to hide a large amount of secret bits into a still image with a high imperceptibility. In this method, data to be embedded are converted into a series of symbols in a notation system with multiple bases. The specific bases used are determined by the degree of local variation of the pixel magnitudes in the host image so that pixels in busy areas can potentially carry more hidden data. The amount of information carried by individual pixels is adapted to the gray value variation in the immediate neighborhood, realized by using a novel multiple-base notational system. As more data are embedded in busy areas and on edges that can tolerate more changes, the method provides a good imperceptibility with a large quantity of embedded data. Ying Wang [20] proposed the purpose of image steganalysis is to detect the presence of hidden messages in cover photographic images. If a steganography method causes someone to suspect that there is secret information in the carrier medium, then this method is considered to have failed. S.R. Khosravirad [21] proposed steganalysis of the random LSB embedding based on the second-order features for images has been defined to be proportional to the rate of LSB alterations, leads to development the feature based steganography. In [22], it has been proposed an introductory idea about edge based steganography and its advantages but not given any idea about selection of an edge detector and role of parameters in extracting the secret message from the stego images. In [23], it has been learned the theoretical and practical overview of digital image processing.

## 3. PROPOSED WORK

In EG-LSB, we use all the edge pixels in a cover image. Here, we first set the parameters (Mean and Standard deviation) for extracting edge. Then we identify the edge pixels by using the Canny Edge detection method. After obtaining the edge pixels, it will hide the data in the 2-bits LSB of the edge pixels only and send the stego image to the receiver. At the receiver, first we find the parameters. Then the canny edge detector is used to identify the edge pixels. We will get same edge pixels at the sender and receiver since we used the same parameters to extract the edge pixels. Thus, we identify the bits where data is hidden. So we extract data from the two LSB bits of the identified edge pixels. Thus, message is obtained. To hide the message, we have proposed the algorithm which is given below:

***Algorithm: EG-LSB – Encoder***
**Input**: Input image: Cover image
Input message: m
**Output**: Stego image

1. Initialize;
2. First we set the parameters (mean and standard deviation) value for edge detector and assign it in the first two pixel
3. For each 2 bits of message
4. For i=1 to *m* do
5. For j=1 to n do
6. If (Edge (Cover image) ==1) then hide two bits of the message in Cover image (i, j) pixel
7. End
8. End
9. End

*Algorithm: EG-LSB – Decoder*
**Input**: Stego image
**Output**: Message m

1. Initialize;
2. First we find the parameters (mean and standard deviation) value for edge detector and from first two pixels
3. For i=1 to *m* do
4. For j=1 to n do
5. If (Edge (Cover image) ==1) then last 2 bits of Cover image (i, j) pixel
6. Until message m recovered.
7. End
8. End
9. End

General model of above algorithms are also represented in block diagram in given in figure-1.

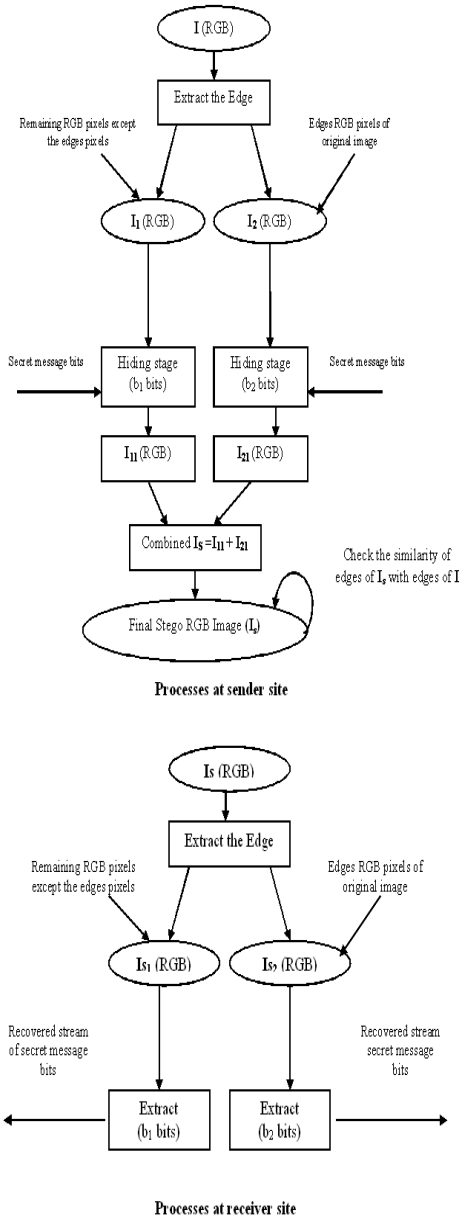


**Figure-1: Block Diagram of EG_LSB**

## 4. RESULTS AND DISCUSSIONS

In this section we are going to discuss result analysis of proposed work. It has implemented this work on MATLAB. There are using mainly three parameters mean, variance for canny edge detector and PSNR ratio for comparing changes of appearance of stego images. There have analyzed this method for picture of Lena which is given in figure-2.

**Figure-2: Experimental Image (Cover Image)**

**Figure-3: Stego Image by (Existing method)**

**Figure-4: Stego Image by EG-LSB (By proposed method)**

**Table-1: Analysis of PSNR by LSB and EG-LSB method on different images**

| S. No | No. of bits | PSNR by LSB | PSNR by EG-LSB |
|---|---|---|---|
| 1 | 4054 | 53.63 | 59.58 |
| 2 | 4524 | 54.85 | 58.69 |
| 3 | 4786 | 50.87 | 54.13 |
| 4 | 5090 | 56.89 | 58.22 |
| 5 | 5624 | 55.36 | 57.62 |
| 6 | 7016 | 52.26 | 57.01 |
| 7 | 7676 | 53.63 | 56.17 |
| 8 | 8162 | 53.03 | 55.95 |
| 9 | 9088 | 52.96 | 55.55 |
| 10 | 9514 | 52.32 | 55.32 |
| 11 | 11200 | 51.69 | 54.71 |
| 12 | 11518 | 51.39 | 54.46 |
| 13 | 11820 | 51.56 | 54.51 |
| 14 | 11910 | 51.04 | 54.36 |
| 15 | 13004 | 50.99 | 54.1 |
| 16 | 13388 | 50.91 | 53.82 |
| 17 | 36854 | 53.62 | 56.64 |

**Table-2: Analysis of PSNR by LSB and EG-LSB method on different images**

| Method | Image size | Size(m) in | PSNR |
|---|---|---|---|
| LSB | 512*512 | 36584 | 51.1262 |
| EG-LSB | 512*512 | 36584 | 54.2244 |

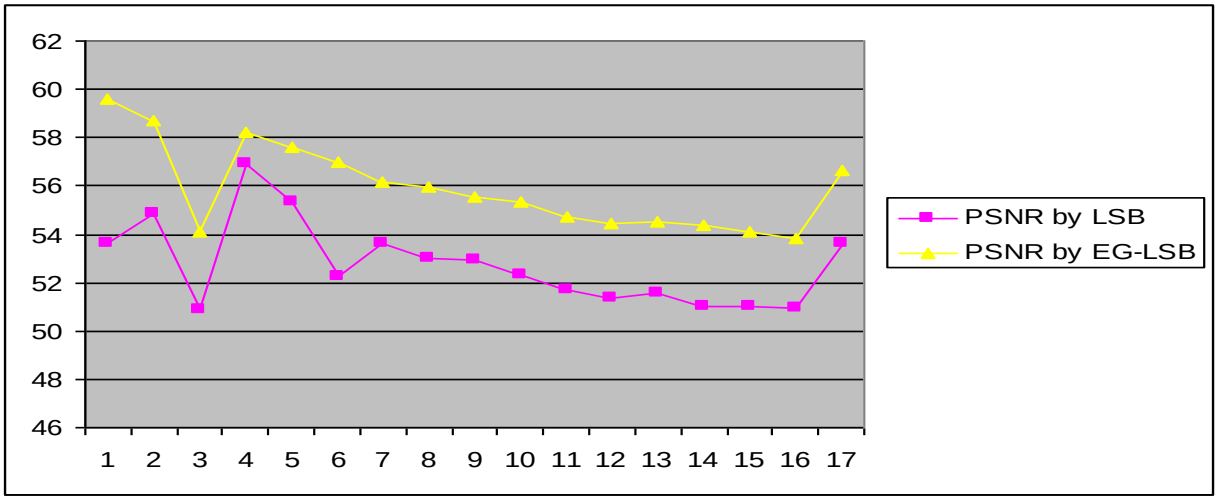


**Figure-5: Comparisons of PSNR by LSB and EG-LSB method on different images.**

For the same length of the message, PSNR of EG-LSB is greater than the PSNR of LSB method, i.e. embedding rate in improved method is larger than the LSB method. It has also given a graph in figure-5 of PSNR ratio by existing and proposed method by selecting several gray scale images. Some data of images and PSNR ratio are also given in table-1. The edge based steganography is to embed secret data in the position of edge pixels, which meets the requirements of both in perception and robustness. The edge based steganography includes algorithms encoding and decoding process respectively. We have used several gray scale images for comparison on existing and proposed LSB embedding techniques. Figure-2 is the original gray scale cover image while figure-3 and figure-4 are the gray-scale stego image by existing LSB and proposed EG-LSB methods respectively. Clearly, It can see that figure-4 has less distortion than figure-3 in the reference of PSNR ratio given in table-2.

## 5. CONCLUSION

EG-LSB approach can also be integrated to color cover images because each three 8-bits component of color images behaves as gray scale images. After performing the above analysis it can be concluded that the proposed method is very effective against steganalysis. This conclusion can be drawn based on obtaining larger PSNR ratio as compared to other methods for same input. Our eye is sensitive to change in both, the brightness and the chrominance but cannot make a precise the comparison of the differences of their values of these two parameters of same image from time to time. Hence it is also the scope of research to generate new parameters in the place of PSNR for comparing similarities in these types of work. In this way, it can be concluded that the proposed work can be enhanced by considering embedding rate and strength against steganalysis attack.

## 6. REFERENCES

[1] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on LSB matching revisited," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 201–214, 2010.

[2] R. Chandramouli and N. Memon, "Analysis of LSB based Image Steganography", IEEE ICIP, pp. 1022-1022, Oct. 2001.

[3] R.J. Anderson, F.A.P. Petitcolas, "On The Limits of Steganography", IEEE Journal of Selected Area in Communications, pp. 474-481, May 1998.

[4] N.F. Johnson, S. Jajodia, "Staganalysis: The Investigation of Hiding Information", IEEE, pp. 113-116, 1998.

[5] K. Rabah, "Steganography- the Art of Hiding Data", Information Technology of Journal 3(3), pp.245-269, 2004.

[6] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", Computer 31, pp.26-34, 1998.

[7] F.A.P. Petitcolas, R.J. Anderson and M.G. Kuhn, "Information Hiding - A Survey", IEEE Proc., Special Issue on Protection of Multimedia Content, 87(7), pp.1062-1078, July 1999.

[8] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing, pp. 75-80, May-Jun 2001.

[9] K. Maney, "Bin Laden's Messages could be Hiding in Plain Sight", USA Today 19 December, 2001.

[10] N. Provos, P. Honeyman, "Detecting Steganography Content on the Internet". CITI Technical Report 01-11, Oct-09, 2001.

[11] N. Provos, "Probabilistic Methods for Improving Information Hiding", CITI Technical Report 01-1, January 31, 2001.

[12] N.F. Johnson & S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software", In Proceeding for the Second Information Hiding Workshop, Portland 0 region, USA, April 1998, pp. 273-289.

[13] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis", IEEE transactions on signal processing, vo1.51, no. 7, Ju1.2003.

[14] Andrew D. Ker, "Steganalysis of LSB Matching in Gray scale Images" , IEEE signal processing letters, vol. 12, no. 6, pp. 441-444, Jun. 2005.

[15] Qinhua Huang and Weimin Ouyang, "Protect Fragile Regions in Steganography LSB Embedding", 3rd International Symposium on Knowledge Acquisition and Modelling, 2010.

[16] Andrew D. Ker, "A General Framework for Structural Steganalysis of LSB Replacement", in Proc.7th Int. Workshop on Information Hiding, 2005, vo1.3427, pp. 296-311.

[17] Adel Almohammad and Gheorghita Ghinea, "Image Steganography and Chrominance Components", 10th IEEE International Conference on Computer and Information Technology, 2010.

[18] Jarno Mielikainen, "LSB Matching Revisited", IEEE signal processing letters, vol. 13, no. 5, May 2006.

[19] Xinpeng Zhang and Shuozhong Wang, "Steganography Using Multiple Base Notational System and Human Vision Sensitivity", IEEE signal processing letters, vol. 12, no. 1, Jan. 2005.

[20] Ying Wang, Student Member, IEEE, and Pierre Moulin, Fellow, IEEE, "Optimized Feature Extraction for Learning-Based Image Steganalysis" IEEE transactions on information forensics and security, vol. 2, no. 1, Mar. 2007.

[21] S.R. Khosravirad, T. Eghlidos and S. Ghaemmaghami, "Closure of sets: a statistically hypersensitive system for steganalysis of least significant bit embedding", IET Signal Process, vol. 5, Iss. 4, pp. 379–389, 2011.

[22] K. Naveen Brahma Teja, Dr. G. L. Madhumati and K. Rama Koteswara Rao, "Data Hiding Using EDGE Based Steganography", International Journal of Emerging Technology and Advanced Engineering, vol. 2, Issue 11, Nov. 2012.

[23] Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing Using MATLAB", Third Edition.

[24] http://www.sarc-wv.com/about_steganography