International Journal of Recent Research and Review, Vol. VI, Issue 3, December 2013

ISSN 2277 – 8322

Improvement in LSB Image Steganography using Message Partitioning

Kazi Azizuddin Rafiuddin[1], Chetan Kumar[2]

M.Tech Student, Assistant Professor, Department of CSE, KITE, Jaipur, India

Email: Email: ramkishan.bairwa@gmail.com

Abstract- Steganography is the art and science of hiding information within other information in such a way that it is hard or even impossible to tell that it is there. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. Security of any Steganography method depends on the quality of image after hiding information inside the image. Qualities of stego image (resultant image) depend on the value of Peak Signal to noise ratio, Signal to noise ratio and number of LSB Changed. Simple Least Significant Bit (LSB) Steganography technique is the most used technique to hide secret information in the least significant bit of the pixels in the stego-image. But a proposed LSB Method divides the secret message into number of partitions, that have same length (number of characters), and find the best LSBs of pixels in the stego-image that are matched to each partition. The main purpose of this method is to minimize the number of LSBs that are changed This will lead to increase the value of PSNR and improve the quality of stego image and as result increase the immunity of the stego-image against the visual attack. The experiment shows that the proposed technique gives good improvement in result as compare to the Classic Least Significant Bit (LSB) technique.

***Keywords* - Hiding information, Image, text hiding, Image Steganography, Steganoanalyst, partitioning and Improvement.**

I. INTRODUCTION

Since the rise of the Internet is one of the most important factors of information technology and communication. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called Steganography.

Steganography is the art and science of hiding information within other information in such a way that it is hard or even impossible to tell that it is there. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. The word Steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing" defining it as "covered writing". In image Steganography the information is hidden exclusively in images.

Steganography differs from cryptography in the sense that, where cryptography focuses on keeping the contents of a message secret, Steganography focuses on keeping the existence of a message secret [1]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. 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 amplified by combining it with cryptography. A successful attack on a Steganography system consists of an adversary observing that there is information hidden inside a file.

II. LITERATURE REVIEW

An overview of image steganography, its uses and its techniques have been discussed in this section. We also attempt to identify the requirements of a good steganographic algorithm and briefly reflect which steganographic techniques are more suitable for which applications. Where one technique (Patchwork) lacks in payload capacity, the other (LSB in BMP) lacks in robustness [2].

Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters

This paper analyzes the various techniques using the various parameters. In this paper LSB, Local Pixel Adjustment Method, Optimal Pixel Adjustment methods are analyze based upon Image Quality.6th ,7th ,8th bit method (85.43 %) and parity checker method (99.41%) are analyze based upon chances of message insertion PVD, Tri –Way PVD (Larger message capacity) methods are analyze based upon Message Length [3].

Comparative study of various Techniques Employed in Image Steganography

Diverse techniques are invented for hiding, LSB technique is an easiest way to implement but 10-15% can have hiding capacity, BPCS (Bit Plane Complexity Segmentation) capacity of hiding. MBPIS (Multi Bit Plane Image Steganography) technique can be used for hiding and exploit the effect of non-random changes by statistical analysis method [4].

Steganography Using Least Significant Bit Algorithm

This paper gives a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hiding the data into image which is implemented through the Microsoft .NET framework. The application creates a stego image in which the personal data is embedded and is protected with a password which is highly secured. The security using Least Significant Bit Algorithm is good but improves the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption [5].

A New Method in Image Steganography with Improved Image Quality

The results of the proposed and LSB hiding methods are discussed and analyzed based on the ratio between the number of the identical and the non identical bits between the pixel color values and the secret message values. The proposed method is efficient, simple and fast it robust to attack and improve the image quality, hence it obtained an accuracy ratio of 83%.Features that could be added to this project include support for file types other than bitmap, and implementation of other steganographic methods [6].

Application of LSB Based Steganographic Technique for 8-bit Color Images

Altering the LSB will only cause minor changes in color, and thus is usually not noticeable to the human eye. This paper presents the results of research investigating the combination of image compression and steganography. The technique developed starts with a 24-bit color bitmap file, and then compresses the file by organizing and optimizing an 8-bit color map. After the process of compression, a text message is hidden in the final, compressed image [7].

Enhanced Least Significant Bit algorithm For Image Steganography

Enhanced Least Significant Bit (ELSB). It improves the performance of the LSB method because information is hidden in only one of the three colors that is BLUE color of the carrier image. This minimizes the distortion level which is negligent to human eye [8].

Image Steganography Using LSB and Edge – Detection Technique

In this paper search how the edges of the images can be used to hiding text message in Steganography .It give the depth view of image steganography and Edge detection Filter techniques. This approach hides the text in selected dark places but the data is not put directly in those pixels and put in low bits of each eight bit pixel [9].

III. CLASSIC LSB IMAGE STEGANOGRAPHY TECHNIQUE

Message

⇩

Convert Message into Binary Form

⇩

Select Suitable Cover Image to Embed Message

⇩

Find LSB of Cover Image

⇩

Insert Message Bit into LSB of Cover Image

⇩

Stego Image

The popular and oldest method for hiding the message in a digital image is the LSB method. In LSB method hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel.

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object is degraded more, and therefore it is more detectable. Other variations on this technique include ensuring that statistical changes in the image do not occur. Some intelligent software also checks for areas that are made up of one solid color. Changes in these pixels are then avoided because slight changes would cause noticeable variations in the area .While LSB insertion is easy to implement, it is also easily attacked. Slight modifications in the color palette and simple image manipulations will destroy the entire hidden message.

One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position. Also it not immune to noise and compression technique.

IV. PROPOSED LSB IMAGE STEGANOGRAPHY TECHNIQUE

Hiding Operation

Message

⇩

Convert Message into Binary Form

⇩

Divide Message bits into number of equal Partitions

⇩

Select Suitable Cover Image to Embed Message

⇩

Find LSB of Cover Image

⇩

Find Best Match Sequence of LSB with bits of Partitions

⇩

Insert Message Bit into LSB of Cover Image

⇩

Stego Image

Extraction Operation

Read Stego Image

⇩

Reconstruct Partitions of Secret Message

⇩

Reassembling all the Partitions to Regenerate Secret Message

⇩

Original Message

Before listing the steps of the algorithm that describe the operations of the proposed technique, some data structures used in the algorithm are defined below:

1) Msg: It consists of binary form of all characters in secret message. The size of msg is n*8 where n is no. of characters in the secret message.
2) Img: It is a list of the Least Significant Bit (LSB) of all pixels in the cover-image.

	Simple LSB Method	LSB with Message Partitioning	
Partition Length	------	2	4
Image	rocket.bmp	rocket.bmp	rocket.bmp
Image Size	256 x 256	256x256	256x256
Message(no. of char)	100	100	100
No. of LSB Changed	347	26	213
PSNR of Stego Image	70.8923	82.1459	73.0118
Time(Hide) seconds	0.156000	4.656000	4.484000
Time(extract) seconds	0.156000	0.016000	0.000000

3) Partition Length: It is a non negative integer number between (2…(n*8)/2) which represents the length of each partition
4) Partition List: It is a list of partitions that is created from the Msg by splitting it to r partitions, where r= (n*8) / Partition Length. Each partition consists of the same number of bits.
5) Index: is a list of indices, each index represents the first index of a sequence of bits in Img which have a best match with the bits for one of the partition in Partition List. There is no overlapping between the matched bits sequences in this technique.

In this method message bits are divided into partitions using proper partition length (like2, 4, 8 etc). Create the partitions in such a way that it consists of equal number of bits in each partition. Select suitable cover image enough to embed entire message. For testing purpose I had used bmp type image of 8 bit depth. Store partitions into one list called partition list. Find all least significant bits of cover image and store into one dimensional array called img. Now find the best match sequence of lsb in one partition with sequence of img. If match is found then replace that sequence of lsb with message bits of partition. If match is not found then insert message bits into lsbs without overlapping the sequence of lsb .Repeat this process for all partitions. Resultant image is called stego image. To extract message follow algorithm for extracting operation.

For Implementation I took lena.bmp (Bit Depth-8bit) and rocket.bmp (Bit Depth-8bit)

Lena.bmp

rocket.bmp

V. EXPERIMENTAL RESULTS

After implementation of Simple and Proposed LSB method for lena.bmp in Matlab following results are obtained.

After implementation of Simple and Proposed LSB method for rocket.bmp in Matlab following results are obtained.

Results are also compared visually. There is no visual change in Cover and Stego Image.

VI. CONCLUSION

	Simple LSB Method	LSB with Message Partitioning	
Partition Length	------	2	4
Image	lena.bmp	lena.bmp	lena.bmp
Image Size	256 x 256	256x256	256x256
Message(no. of char)	100	100	100
No. of LSB Changed	351	17	200
PSNR of Stego Image	70.8425	83.99	73.2853
Time(Hide) seconds	0.157000	5.813000	4.703000
Time(extract) seconds	0.157000	0.016000	0.015000

The Proposed LSB Method divides the long secret message into number of short equal partitions. Then hide these short partitions in different parts of the best matched LSB in the pixels of the stego-image. The main purpose of this method is to decrease the number of LSB that are changed and as a result increase the immunity of the stego-image against the attack by human visual system (HVS). The problem of the proposed LSB Method is time required to hiding message that is spend during the search to find the best matching when using a large size stego-image.From the experiments I conclude that the proposed LSB image steganography technique success in increase the security of the secret message that is hide in the stego-image by decreasing the number of LSB that are changed in the pixels of the stego-image. Also with the Comparison PSNR value we conclude that proposed LSB Method gives best Result as compare to classic LSB algorithm.

VII. REFERENCES

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

[2] T. Morkel, J.H.P. Eloff, M.S. Olivier, An Overview of Image Steganography Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science. University of Pretoria, 0002, Pretoria, South Africa

[3] Rajkumar Yadav, Analysis of Incremental Growth in Image Steganography Techniques for Various Parameters, Int. J. Comp. Tech. Appl., Vol 2 (6),1867-1870

[4] Preeti Singh, Charu Pujara, Comparative study of various Techniques Employ in Image Steganography, International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012

[5] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, Steganography Using Least Significant Bit Algorithm, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May- Jun 2012, pp. 338-341

[6] Atallah M. Al-Shatnawi, A New Method in Image Steganography with Improved Image Quality. Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915

[7] Mamta Juneja, Parvinder S. Sandhu, Ekta Walia, Application of LSB Based Steganographic Technique for 8-bit Color Images. World Academy of Science, Engineering and Technology 50 2009

[8] Shilpa Gupta, Geeta Gujral and Neha Aggarwal, Enhanced Least Significant Bit algorithm For Image Steganography, IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230

[9] Nitin Jain, Sachin Meshram, Shikha Dubey, Image Steganography Using LSB and Edge – Detection Technique, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 223