Implementation of LSB Steganography and its Evaluation for Various File Formats

V. Lokeswara Reddy
Department of CSE, K.S.R.M. College of Engg., Kadapa, A.P. India
Email: vl_reddy@yahoo.com
Dr. A. Subramanyam
Dept. of CSE, AITS, Rajampet, Y.S.R.(Kadapa) Dist.. A.P.
Dr.P. Chenna Reddy
Dept. of CSE, JNTUCE, Pulivendula, Y.S.R.(Kadapa) Dist.. A.P.

---**ABSTRACT**---

Steganography is derived from the Greek word steganos which literally means "Covered" and graphy means "Writing", i.e. covered writing. Steganography refers to the science of "invisible" communication. For hiding secret information in various file formats, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. The Least Significant Bit (LSB) embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-Bit, 8-Bit, Gray scale format. This paper explains the LSB Embedding technique and Presents the evaluation for various file formats.

Keywords***:* Steganography, Least Significant Bit (LSB), GIF, PNG, BMP.**

Date of Submission: 24, August 2010 Date of Acceptance: 08 November 2010

I. INTRODUCTION

Digital content is now posing formidable challenges to content developers, aggregators, distributors and users. The destruction, extraction or modification of the embedded message is required to develop more robust systems so that the digital content processing and organization becomes easy.

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.

The shift from cryptography to stegnography is due to that concealing the image existence as stegno-images enable to embeded the secret message to cover images. Steganography conceptually implies that the message to be transmitted is not visible to the informal eye. Steganography has been used for thousands of years to transmit data without being intercepted by unwanted viewers. It is an art of hiding information inside information. The main objective of Steganography is mainly concerned with the protection of contents of the hidden information. Images are ideal for information hiding[1,2] because of the large amount of redundant space is created in the storing of images. Secret messages are transferred through unknown cover carriers in such a manner that the very existence of the embedded messages is undetectable. Carriers include images; audio, video, text or any other digitally represented code or transmission. The hidden message may be plaintext, cipher text or anything that can be represented as a bit stream.

II. IMAGE STEGANOGRAPHY

Image compression techniques are extensively used in steganography. Among the two types of image compressions, lossy compression and loss less compression; lossless compression formats offer more promises. Lossy compression compression may not maintain the original image's integrity. Lossless compression maintains the original image data exactly, hence it is prefered. Example of Lossy compression format is JPEG format files. Examples of Lossless compression formats are GIF[3] and BMP formats.

We have used an 8-bit image size for implementation of our steganography. Improvement in stegnographic techniques is make it possible to apply the Detecting LSB Steganography in Colour and Gray- Scale Images which were confined to gray scale images in the initial stages The difficulty in colour images control is solved later on in many techniques such as the analysis of the variation of the gradient energy. The secret message embedded in the target image is detected in both gray and colour images, and the length of the embedded message is estimated [5, 6].

III. HIDING METHODS IN IMAGE STEGANOGRAPHY

In Image Steganography, There are a variety of methods using which information can be hidden in images.

Least Significant Bit Replacement Technique: In image steganography almost all data hiding techniques try to alter insignificant information in the cover image. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. For instance, a simple scheme proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image[7,8,9] . The altered image is called stego-image. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc. We will be emphasizing more on this technique for the various image formats.

Moderate Significant Bit Replacement Technique:
The moderate significant bits of each pixel in the cover image can be used to embed the secret message. This method improves sensitivity to modification, but it degrades the quality of stego-image.

Experiments have shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision.

IV. THE LSB TECHNIQUE

The least significant bit i.e. the eighth bit inside an image is changed to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components, since they are each represented by a byte. An 800×600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. As an example, suppose that we have three adjacent pixels (9 bytes) with the RGB encoding.

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

When the number 300, can be which binary representation is 100101100 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in **bold** have been changed)

10010101 0000110**0** 1100100**0**
1001011**1** 0000111**0** 11001011
10011111 00010000 1100101**0**

Here the number 300 was embedded into the grid, only the 5 bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. The human eye cannot perceive these changes - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the LSB without noticing the difference[10].

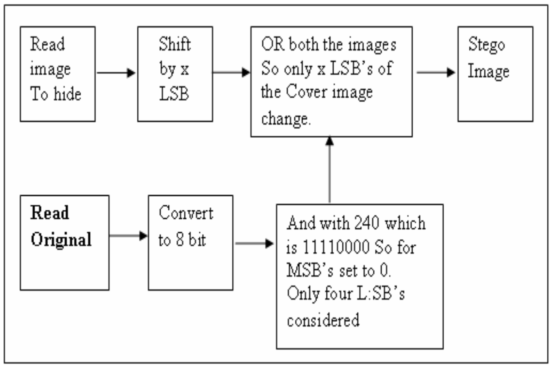

Read image To hide
Shift by x LSB
OR both the images So only x LSB's of the Cover image change.
Stego Image
Read Original
Convert to 8 bit
And with 240 which is 11110000 So for MSB's set to 0. Only four L:SB's considered

Fig.1 Block Diagram for implemented Logic of LSB embedding

V. DESIGN DETAILS

This section focuses on algorithms of LSB Steganography and Steganalysis[10]

A. Algorithm for Hiding (Steganography)

1. Read the original image and the image which is to be hidden in the original image
2. Shift the image to hide in the cover image by X bits.
3. And the original image or cover image with 240 which is 11110000 So four MSB's set to 0. Because of this only four LSB's considered further.
4. The shifted hidden image and the result of step 3 are bitored. This makes changes only in the X LSB bits so that the image is hidden in the original image.

In MATLAB we convert it to unit8 format. This image can be called as the stego image

B. Algorithm for Steganalysis

1. The stego image is bit shifted by 4 bits since it was shifted by 4 bits to insert it into the original image.
2. The image is the ANDED with 255 i.e., 11111111, which gives the original image. It is ANDED with 255 because initially all the LSB's were made 0. Now it is recovered back.
3. To get it to Unit8 format we, convert it back to unit8 which is the extracted image.

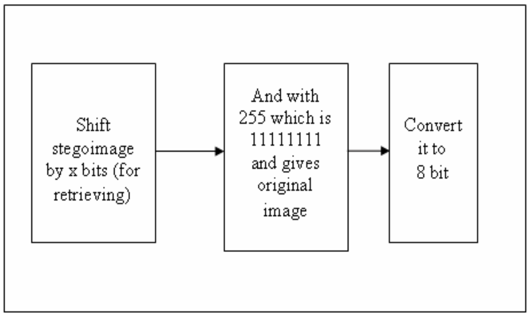

Shift stegoimage by x bits (for retrieving)
And with 255 which is 11111111 and gives original image
Convert it to 8 bit

Fig. 2: Block Diagram for Steganalysis

VI. IMAGE ANALYSIS

A. LSB in BMP

The BMP file format also called bitmap or DIB file format (for *device-independent bitmap*), is an image file format used to store bitmap digital images.Since BMP is not widely used the suspicion might arise, if it is transmitted with an LSB stego. When image are used as the carrier in Steganography they are generally manipulated by changing one or more of the bits of the byte or bytes that make up the pixels of an image. The message can be stored in the LSB of one colour of the RGB value or in the parity bit of the entire RGB value. A BMP is capable of hiding quite a large message. LSB in BMP is most suitable for applications, where the focus is on the amount of information to be transmitted and not on the secrecy of that information. If more number of bits is altered, it may result in a larger possibility that the altered bits can be seen with the human eye. But with the LSB the main objective of Steganography is to pass a message to a receiver without an intruder even knowing that a message is being passed is being achieved.

B. LSB in PNG

Portable Network Graphics (PNG) is a bitmapped image format that employs lossless data compression. PNG was created to improve upon and replace GIF. Since PNG is widely used the suspicion might not arise if it is transmitted with an LSB stego. When images are used as the carrier in Steganography they are generally manipulated by changing one or more of the bits of the byte or bytes that make up the pixels of an image. The message can be stored in the LSB of one colour of the RGB value or in the parity bit of the entire RGB value .A PNG is capable of hiding quite a large message. LSB in PNG is most suitable for applications where the focus is on the amount of information to be transmitted and not on the secrecy of that information. If more number of bits is altered it may result in a larger possibility that the altered bits can be seen with the human eye. But with the LSB the main objective of steganography is to pass a message to a receiver without an intruder even knowing that a message is being passed is being achieved.

C. LSB in GIF

Graphics interchange format also known as GIF is one of the machine independent compressed formats for storing images. Since GIF images only have a bit depth of 8, amount of information that can be hidden is less than with BMP. Embedding information in GIF images using LSB results in almost the same results as those of using LSB with BMP. LSB in GIF is a very efficient algorithm to use when embedding a reasonable amount of data in a grayscale image. GIF images are indexed images where the colours used in the image are stored in a palette. It is sometimes referred to as a colour lookup table. Each pixel is represented as a single byte and the pixel data is an index to the colour palette. The colours of the palette are typically ordered from the most used colour to the least used colours to reduce lookup time. Some extra care is to be taken if the GIF images are to be used for Steganography. This is because of the problem with the palette approach. If the LSB of a GIF image is changed using the palette approach, it may result in a completely different colour. This is because the index to the colour palette is changed. The change in the resulting image is noticeable if the adjacent palette entries are not similar. But the change is not noticeable if the adjacent palette entries are similar. Most applications that use LSB methods on GIF images have low security because it is possible to detect even moderate change in the image. Solutions to these problems could be

1. Sort the palette so that the colour difference between consecutive colours is minimized
2. Add new colours, which are visually similar to the existing colours in the palette.
3. Use Gray scale images. In a 8 bit Gray scale GIF image, there are 256 shades of gray. This results in gradual changes in the colours and it is hard to detect.

VII. EXPERIMENTED RESULTS

Following experimental results highlights on 8 bit LSB Steganography.

A. Results for .png image

Cover Image

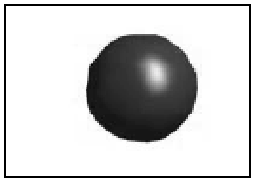
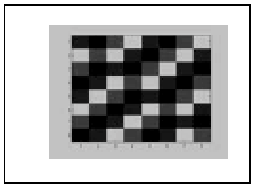
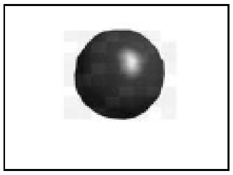


Image to hide

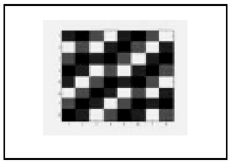


8 bit stego image

Stego image



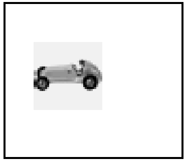
Recovered image



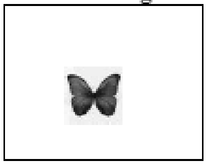
B. Results for .bmp file

8 bit stego image

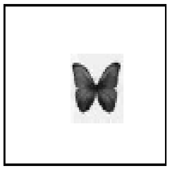
Message



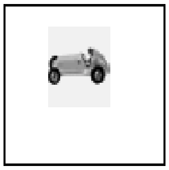
Cover image



Stego



Recovered



VIII. EVALUATION OF IMAGE QUALITY

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio[3] and histogram.

A. Mean-Squared Error

The mean-squared error (MSE) between two images $I_1(m,n)$ and $I_2(m,n)$ is:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

M and *N* are the number of rows and columns in the input images, respectively. Mean-squared error depends strongly on the image intensity scaling. A mean-squared error of 100.0 for an 8-bit image (with pixel values in the range 0-255) looks dreadful; but a MSE of 100.0 for a 10- bit image (pixel values in [0,1023]) is barely noticeable

B. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image, but between-image comparisons of PSNR are meaningless. MSE and PSNR values for each file format is shown in table 1.

Table 1: Image quality metrics for bmp file

	Cover image	Stego image	Cover- Stego image
MSE	224.948	244.162	69.826
PSNR	24.6100	24.2540	29.690

IX. EVALUATION OF DIFFERENT TECHNIQUES

There are many steganographic algorithms available. One should select the best available algorithm for the given application. Following characteristics are to be evaluated while selecting a particular file format for Steganography. Steganography says that the secret message is to be hidden and it should result in an distortion less image. The distortion must not be visible to the human eye. The amount of data embedded in the image also plays an important role. The algorithm decides how much amount of data could be embedded in the image resulting in a distortion less image. Steganalysis is the technique of detecting the hidden information in the image. The algorithm for Steganography must be such that the steganalysis algorithms should fail. i.e the Steganography algorithms must not be prune to attacks on steganalysis. During communication the intruder could check the original image to remove the hidden information.. He/she may manipulate the image. This manipulation may include cropping or rotation etc of the images. The manipulations done may cause the image distortion. Steganographic algorithms chosen must be such that it overcomes such manipulation and the steganographic data reaches the destination in the required format.

Table 2: Comparison of LSB technique for various file formats

	LSB In BMP	LSB in GIF	LSB In PNG
Percentage Distortion less resultant image	High	Medium	High
Invisibility	High	Medium	Medium
Steganalysis detection	Low	Low	Low
Image manipulation	Low	Low	Low
Amount of embedded data	High	Medi um	Medium
Payload capacity	High	Medi um	Medium
Independent of file format	Low	Low	High

X. CONCLUSION

Since BMP uses lossless compression, LSB makes use of BMP image. To be able to hide a secret message inside a BMP file, one would require a very large cover image. BMP images of 800×600 pixels found to have less web applications. Moreover such uses are not accepted as valid. For this reason, LSB Steganography has also been developed for use with other image file formats. Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. LSB in GIF images has the potential of hiding a large message, but only when the most suitable cover image has been chosen.

References

[1] Pfitzmann Birgit. Information Hiding Terminology, First International Workshop, Cambridge, UK, Proceedings, Computer Science, 1174. pp. 347-350, May–June.

[2] Westfield Andreas and Andreas Pfitzmann, Attacks on Steganographic Systems, Third International Workshop, IH'99 Dresden Germany, October Proceedings, Computer Science 1768. pp. 61- 76, 1999.

[3] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Science*, Silman, J., "Steganography and Steganalysis: An Overview", *SANS Institute*, 2001 Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999.

[4] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*, February 1998.

[5] Li Zhi,Sui Ai Fen., "Detection of Random LSB Image Steganography" The IEEE 2003 International Symposium on Persona1,lndoor and Mobile Radio Communication Proceedings, 2004.

[6] Jessica Fridrich, Miroslav Goljan, and Rui Du., "Detecting LSB Steganography in Color and Gray-Scale Images", - IEEE Multimedia.

[7] F.Collin,\Encryptpic," http://www.winsite.com/bin/ Info?500000033023.

[8] G. Pulcini, \Stegotif," http://www.geocities.com /SiliconValley/9210/gfree.html.

[9] T. Sharp, \Hide 2.1, 2001,"www.sharpthoughts. org.

[10] Deshpande Neeta, Kamalapur Snehal, Daisy Jacobs "Implementation of LSB Steganography and Its Evaluation for Various Bits" Digital Information Management, 2006 1st International conference.pp 173-178,2007.

Authors Biography

V.Lokeswara Reddy did his M.Tech (CSE) from SRM University, Chennai in the year 2005. He did his M.C.A from S.V. University, Tirupati in the year 2000. He is pursuing his Ph.D from JNTUA, Anantapur. He has a total of 09 years of experience in teaching. Currently he is working as Associate Professor at K.S.R.M College of Engineering, Kadapa. He has presented 2 papers in International and National Conferences.

Dr.A.Subramanyam received his Ph.D. degree in Computer Science and Engineering from JNTU College of Engineering, Anantapur. He has obtained his B.E.(ECE) from University of Madras and M.Tech.(CSE) from Visweswaraiah Technological University. He is having 17 years experience in teaching. He is currently working as Professor & HOD in the Department of Computer Science and Engineering of Annamacharya Institute of Technology & Sciences, Rajampet, Y.S.R.(Kadapa) Dist. A.P. He has presented and published number of papers in International and National Conferences, International and National Journals. He is guiding few Ph.D.s. His research areas of interest are parallel processing, network security and data warehousing.

Dr. P. Chenna Reddy did his B.Tech (CSE) from S.V. University College of Engineering, Tirupati in the year 1996. He did his M.Tech from JNTU, Anantapur. He completed his Ph.D from JNTU, Hyderabad. He has a total of 13 years of experience in teaching. Currently he is working as Associate Professor at JNTUA College of Engineering, Pulivendula, Y.S.R.(Kadapa) Dist., A.P. He has number of publications to his credit.