International Journal of Computational Intelligence and Informatics, Vol. 3: No. 3, October - December 2013

Evaluation of LSB Based Image Steganography Technique for various File Formats

K Thangadurai
PG and Research Department of Computer Science
Government Arts College (Autonomous),
Karur, TamilNadu,India.
ktramprasad04@yahoo.com

G Sudha Devi
PG and Research Department of Computer Science
Government Arts College (Autonomous),
Karur, TamilNadu, India.
gsudha.cheran@gmail.com

***Abstract*- Steganography is derived from the Greek word steganos which literally means "Covered" and graphy means "Writing", i.e. covered writing. Steganography is the art and science of hiding messages in such a way that no one apart from sender and receiver identify the message. The paper describes the steganalysis technique for the detection of secret message in the image. The strong and weak point of this technique is mentioned briefly. Steganography function is used to hide a secret message in any media such as text, image, audio and video. There are many algorithms used for hiding the information. One of the simplest and best known techniques is Least Significant Bit (LSB). This paper focuses on image Steganography and hiding the message in the Least Significant Bit (LSB) method. We also discuss the LSB method used for various file formats.**

Keywords- Cryptography, Steganography, Steganalysis, LSB (Least Significant Bit), GIF, PNG, BMP.

I. INTRODUCTION

Cryptography is a technique used to secure the secrecy of information and many different methods have been developed to encrypt and decrypt data in order to keep the message secret [10]. 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 [1, 20].

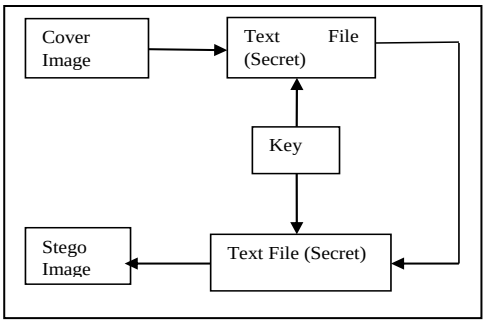

Figure 1. Steganography process

Steganography refers to information or a file that has been concealed inside a digital picture, video or audio file [5]. If a person views the object he or she will have no idea that there is any hidden information. Therefore the person will not try to decrypt the information [22]. The Fig.1 shows the Steganography process.

The cryptography and Steganography are closely related. The comparison between cryptography and Steganography is illustrated from the following Table I.

TABLE I. CRYPTOGRAPHY VERSUS STEGANOGRAPHY

Cryptography	Steganography
Known message passing	Unknown message passing
Encryption prevents an unauthorized person from discovering the content of a message communication	Steganography prevents discovery of the existence of message communication
It is common technology	It is little known technology
Most of algorithm known by all	Technology is being developed for certain formats
Cryptography alter the structure of secret message communication	Steganography does not alter the structure of secret message

ISSN: 2349-6363

II. STEGANOGRAPHY

Steganography is the process of hiding secret information in an unsuspicious cover object [4].

A. *Types of steganography*

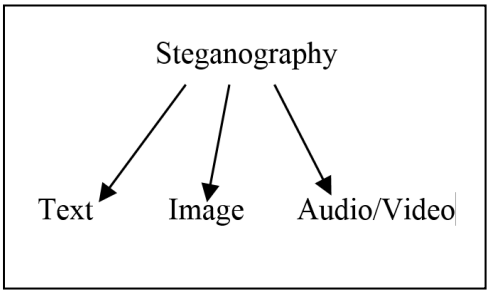

Figure 2.Types of Steganography

Fig.2 shows the various types of steganography techniques.

Text Steganography: Digital files are not used very often because text files have a very small amount of redundant data.

Image Steganography: It is quite simple and secure way to transfer the information over the internet.

Audio/Video Steganography: It is very complex in use [8].

B. *Applications of steganography*

Steganography takes important role in the field of information technology, because it is used for the purpose of network security [2]. It is used for message authentication, that means message is from an authorized sender and it will transmitted to an intended receiver [10, 19]. There will be no modification in content of information during communication, so it keeps data integrity. Steganography technique is used in the field of watermarking. Watermarking is the process of hiding information in a carrier in order to protect the ownership of text, music, films and art [14].

C. *Types of Image Steganography*

a) Transform domain - Jpeg

b) Spread spectrum - Patchwork

c) Image domain - LSB and MSB in BMP, LSB and MSB in JPG

Methods of hiding data in Digital Images

1. LSB (Least Significant Bit): This method is used for hiding data into cover image. The least significant bit of each pixel of an image is altered to a bit of a message that is to be hidden [3, 19].

2. MSB (Most Significant Bit): In this method the MSB bits of each pixel of an image are changed to a bit of a message that is to be hidden [17].

D. *LSB Algorithm*

Algorithm of LSB Based Steganography

Algorithm to embed text message using Grayscale image

Step 1: Read the cover image and text message, which is to be hidden in the cover image

Step 2: Convert text message into binary

Step 3: Calculate LSB of the each pixel of cover image

Step 4: Replace LSB of cover image with each bit of secret message one by one

Step 5: Write stego image

Algorithm to retrieve text message using Grayscale image

Step 1: Read the stego image

Step 2: Calculate LSB of each pixel of stego image

Step 3: Retrieve bits and convert each 8 bit into character

Step 4: Calculate MSE and PSNR

III. STEGANALYSIS PROCESS

Steganalysis is the art of detecting the existence of hidden information. It attempts to defeat the goal of steganography. Tracking criminal activities over the internet, cyber warfare and gathering evidence for investigation are the applications of Steganalysis [3]. Although it is a relatively recent branch compared to steganography, there is an increasing interest to steganalysis. The types of steganalysis techniques are divided into two main groups [12].

A. Detecting Hidden Information (Passive steganalysis)

Passive Steganalysis is the type of steganalysis which aims to detect the presence of a hidden message in a stegoobject, or to detect the steganography tool used to hide the message.

a) Detecting Text steganography

Hiding messages in text files is one of the simplest methods. So, detecting text steganography is also simple one. The hidden characters, lines and extra spaces in a text file can be visible and it can be easily detected [2].

b) Detecting Image Steganography

A steganalysis technique on image files is analyzing many stego-images and their original versions according to color composition, luminance and pixel relationships. By applying LSB method in order to hide a message, randomness occurs in least significant bits of the cover object. And this randomness can easily be detected by statistical analysis of LSB's on the cover object.

c) Detecting file system Steganography

File system Steganography can be detected by using tools which analyze the file system and it report the information hidden on unused partitions.

d) Detecting Steganography on TCP/IP Headers

Internet firewalls can be customized to catch the TCP/IP packet which contains the information in their unused spaces.

B. Defeating Steganograms (Active Steganalysis)

Active Steganalysis covers the techniques used to disable the secret communication, by extracting and damaging the hidden messages. Detecting the message is not always necessary, since the goal of Steganography is already defeated when the existence of the message is detected [3].

a) Disabling Text Steganograms:

The hidden messages in a text file can easily be destroyed by opening the file in a word processor and reformatting the text.

b) Disabling Image Steganograms

Applying JPEG compression on the image is the simplest method of corrupting image. In order to defeat steganograms created by transform domain tools, multiple image processing techniques can be applied. These techniques include cropping, removing portions of the image, rotating the image, adding or removing noise.

c) Disabling Audio and Video steganograms

In steganalysis of audio files, the same technique with image steganalysis is applied. The image and audio steganalysis can be combined and it can be applied on video files.

d) Disabling steganograms in File systems

Hiding messages in file system are not so secure. It is always possible for operating system which does a lot caching and creating of temporary files to overwrite the partitions of file system [12].

e) Disabling steganograms in TCP/IP Headers

The information is embedded in the headers of TCP/IP packets. The information can be catched and filtered by firewalls. So during the routing process it is possible for these headers to be overwritten.

IV. IMAGE

An image is a collection of numbers that constitute different light intencities in different areas of the image. This numeric representation forms a grid and the individual points are referred as pixels [7]. There are many types of image formats used for Steganography and each has certain merits and demerits.

A. GIF Format

GIF is used for storing multiple bitmap images in a single file for exchange between platforms and images. GIF use the lossless LZW compression. It allows only 8-bit indexed color.It is commonly used for images presented on the web.

B. BMP Format

A bitmap file format can be uncompressed or compressed with RLE. BMP file does not support CMYK color. The new version of BMP supports the Alpha channels.

TABLE II. COMPARISON OF GIF AND BMP IMAGES

	GIF	**BMP**
File types	Graphics Interchange format	Windows bitmap
File Suffix	.gif	.bmp
Standard color mode	Index color Grayscale	Index color RGB
Color Depth	8-bit color	1-32 bit color
Compression algorithms	Lossless(LZW)	Lossless(REA)

TABLE III. COMPARISON OF LSB FOR VARIOUS FILE FORMATS

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

V. IMAGE ANALYSIS

A. LSB in GIF

GIF (Graphics Interchange format) is one of the machine independent compressed formats for storing images. LSB in GIF is a very efficient algorithm to use when embedding a reasonable amount of data in a grayscale image [7]. Embedding information using LSB method in GIF images results in almost the same results as those of using LSB with BMP. GIF images are indexed images where the colours used in the image are stored in a palette. Each pixel is represented as a single byte and the pixel data is an index to the colour palette [9]. 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.

B. LSB in PNG

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 [10]. A PNG is capable of hiding quite a large message. 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. 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 [11]. 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 [15].

C. LSB in BMP

The BMP file format also called bitmap file format, is an image file format used to store bitmap digital images. 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[13,18]. 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 method in BMP file format 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.

VI. EVALUATION OF IMAGE QUALITY

A. Mean – Squared Error(MSE)

The mean-squared error (MSE) between two images I1 (m, n) and I2 (m, n) is:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N} \quad (1)$$

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 [16].

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IJCII, CI, PU, pu, ci, and cs do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range [6].

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

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 [23].

VII. CONCLUSION AND FUTURE WORK

Cryptography deals with taking a message and making it appear as random noise, unreadable to an outside world. Steganography is not intended to replace cryptography but supplement it. Steganlaysis is the art of detecting the hidden messages embedded in digital media using steganography. Both Steganography and steganalysis have received a great deal of attention from law enforcement and the media. The paper describes an evaluation of LSB steganography for different file formats. The strong and weak points of these file formats in LSB based image steganography are mentioned briefly. One would require a very large cover image to be able to hide a secret message inside a BMP file. The 800 x 600 pixels of BMP image file found to have less web applications. For this reason, LSB based image steganography is used with other file formats. PNG does not support animation like GIF. PNG works well in online applications such as World Wide Web. LSB in GIF is a very efficient algorithm to use when embedding a reasonable amount of data in a gray scale image. We can hide the data into video files for future work.

ACKNOWLEDGMENT

We would like to thanks to the Principal, HOD and faculty members of P.G and Research Department of Computer Science and Research Scholars Government Arts College (Autonomous), Karur for their encouragement to publish this work.

REFERENCES

[1] M. S. Sutaone, M.V. Khandare, "Image Based Steganography Using LSB Insertion Technique", IET International Conference on Wireless, mobile and multimedia networks, IEEE, Jan 2008.

[2] H.B. Karaman, S.Sagiroglu,"An Application Based on Steganography", IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Aug 2012.

[3] Yam bern Jina Chanu, Themrichon Tuithung, Kh. Manglem Singh, " A Short Survey on Image Steganography and Steganalysis Techniques",3rd National Conference on Emerging Trends and Applications in Computer Science(NCETACS), IEEE, March 2012.

[4] U. T. Tilakaratne, U.A.J.Pinidiyaarachchi, "Image Steganography Scheme Based on Reversible Data Embedding Strategy", The 8th International Conference on Computer Science & Education, IEEE, April 2013.

[5] Ross J.Abderson and Fabien A.P.Petitcolas, "On the limits of steganography", IEEE Journal on selected areas in communications Vol.16, No.4, May 1998.

[6] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain,"A new approach for LSB Based Image Steganography using Secret Key", 14th International Conference on Computer and Information Technology(ICCIT 2011), pp.22-24 , IEEE, December 2011.

[7] Eltyeb E.Abed Elgabar, Haysam A. Ali Alamin,"Comparison of LSB Steganography in GIF and BMP Images", International Journal of Soft Computing and Engineering (IJSCE), Vol-3, Issue-4, September 2013.

[8] Preeti Singh, Charu Pujara," Comparative study of various Techniques Employ in Image Steganography", International Journal of Engineering and Advanced Technology (IJEAT), Vol-1, Issue-5, June 2012.

[9] Pritam Kumari, Chetna Kumar, Preeyanshi, Jaya Bhushan," Data Security Using Image Steganography And Weighing Its Techniques", International Journal of Scientific & Technology Research Volume 2, Issue 11, November 2013.

[10] Namita Tiwari, Dr.Madhu Shandilya," Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", International Journal of Computer Applications, Vol.6, No.2, Sep 2010.

[11] V.Lokeswara Reddy, Dr.A.Subramanyam, Dr.P.Chenna Reddy,"Implementation of LSB Steganography and its Evaluation for Various File Formats,"International Journal of Advanced Networking and Applications", Vol. 02, Issue: 05, pages 868-872. (2011).

[12] Kevin Curran, Karen Bailey," An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, fall 2003, Vol.2, Issue.2.

[13] Vivek Kumar, Sandesh Kumar, Lavalee Singh, Prateek Yadav,"Implementation of LSB Steganography and its Evaluation for Various File Formats (LSB, JSTEG)", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 6, June – 2013.6.

[14] Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", I.J.Modern Education and Computer Science, 2012, 6, 27-34.

[15] Wai Wai Zin, "Message Embedding In PNG File Using LSB Steganographic Technique", International Journal of Science and Research (IJSR), Vol.2 Issue 1, January 2013.

[16] Dr. Ekta Walia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography", Global journal of Computer Science and Technology, Vol. 10, Issue 1 (Ver. 1.0), April 2010.

[17] Prashanti .G, Sandhya Rani.K, Deepthi.S," LSB and MSB Based Steganography for Embedding Modified DES Encrypted Text", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue 8, August 2013.

[18] Mr. Rohit Garg," Comparison of Lsb & Msb Based Steganography In Gray-Scale Images", International Journal of Engineering Research & Technology (IJERT), Vol 1, Issue 8, October 2012.

[19] Deepesh Rawat, Vijaya Bhandari," Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method", International Journal of Computer Applications, Vol.67,No.1, April 2013.

[20] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia, "Application of LSB Based Steganographic Technique for 8-bit Color Images", World Academy of Science, Engineering and Technology 26, 2009.

[21] Namita Tiwari1, Madhu Shandilya, "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth", International Journal of Security and Its Applications, Vol.4, No.4, October 2010.

[22] M.Sivaram, B.DurgaDevi, J.Anne Steffi,"Steganography of two LSB bits", International Journal of Communications and Engineering, Vol.01, Issue 01, March 2012.

[23] Parisa Gerami, Subariah Ibrahim, Morteza Bashardoost , "Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment ",International Journal of Computer Applications , Vol.55,No.2, October 2012.