An analysis of LSB Based Image Steganography Techniques

K.Thangadurai and G.Sudha Devi,
PG and Research Department of Computer Science,
Govt., Arts College (Autonomous), Karur, India.
Email:ktramprasad04@yahoo.com

Abstract— **Steganography refers to information or a file that has been concealed inside a digital picture, video or audio file. If a person views the object in which the information is hidden inside, he or she will have no indication that there is any hidden information. So the person will not try to decrypt the information. Steganography can be divided into Text Steganography, Image Steganography, Audio/Video Steganography. Image Steganography is one of the common methods used for hiding the information in the cover image. LSB is very efficient algorithm used to embed the information in a cover file. This paper presents the detail knowledge about the LSB based image steganography and its applications to various file formats. In this paper we also analyze the available image based steganography along with cryptography technique to achieve security.**

Keywords- Cryptography, Steganography, Message Hiding, Cover Image, LSB, GIF, PNG.

I. INTRODUCTION

Cryptography is a method used for secure communication in the presence of third parties [2]. The various aspects in information security are,

- Confidentiality: The information transmission is only for reading by authorized persons.
- Authentication: The origin of the message is identified correctly with an assurance that the identity is not false.
- Integrity: Only authorized persons can be able to modify transmitted or stored information.
- Non-Repudiation: It requires that neither the sender, nor the receiver of message can be able to deny the transmission.
- Access Control: Requires that access may be controlled by the target system.
- Availability: The computer system assets are available to authorized parties whenever needed.

Steganography is the technique of hiding of text in information like image, text, audio and video [7]. There are different types of Steganography :

i).Text Steganography: It is not used very often because text files have small amount of redundant data.

ii).Image Steganography: This is used widely for hiding information in the cover image.

iii).Audio/Video steganography: Compared to others this is very complex to use [3].

II. CRYPTOGRAPHY AND STEGANOGRAPHY

If the attacker reads the secret message, the system is broken in cryptography [2].The “Fig.1.” shows the combination of cryptography and Steganography

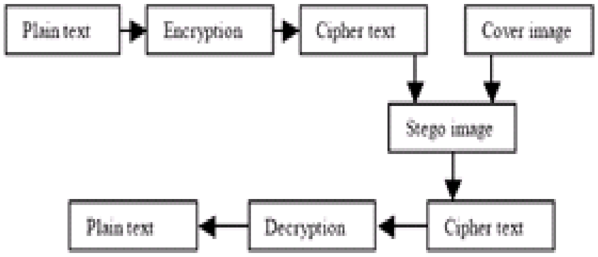

Figure 1. Combination of cryptography and steganography

A. *Cryptography versus Steganography*

There are many differences between Steganography and cryptography. The comparision between Steganography and cryptography is illustrated from the following Table 1.

TABLE I. Comparision between Cryptography and Steganography

Cryptography	Steganography
Known message passing	Unknown message passing
Encryption prevents unauthorized persons from discovering the contents of communication	Steganography prevents the discovery of existence of communication
It is common technology	Little known knowledge technology
Cryptography alters the structure of the secret message	Steganography does not alter the structure of the secret message

978-1-4799-2352-6/14/$31.00 ©2014 IEEE

III. Image Steganography

A. Types of Steganography

The following are the types of steganography in various domains [1].

- Transform domain
  Jpeg
- Spread domain
  Patch work
- Image domain
  LSB and MSB in BMP
  LSB and MSB in JPEG

The steganography process is shown in "Fig.2."

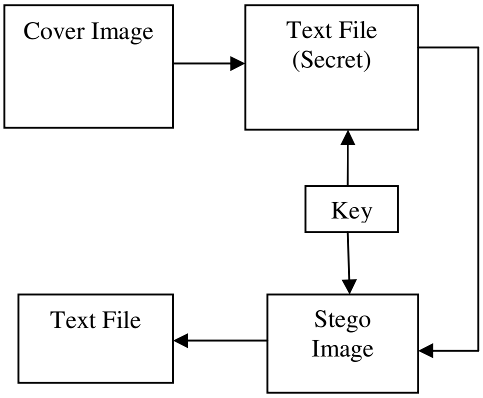

Figure 2. Steganography process

B. Applications of Steganography

Steganography is very useful in the field of information technology for secure communication [3]. It is applicable to the following areas:

- Secret data storing and efficient confidential communication
- Protection of data alteration
- Media Database Systems

It keeps the integrity of data, this means there will not be modification in the content of the information during communication. Steganography technique is also used for watermarking. Watermarking is the process of hiding information in a carrier in order to protect the ownership of text, music, films and art.

C. Cover Image Selection

To hide the secret message in cover image the proper cover image should be selected .It is very important to hide the information in digital image using lossless compression algorithm, because there is a chance for losing of information at the time of communication. The "Fig.1" shows the process of cover image selection. It provides chance for selecting the proper cover image that should be suitable for hiding the message [9]. The "Fig.3" shows the cover image selection

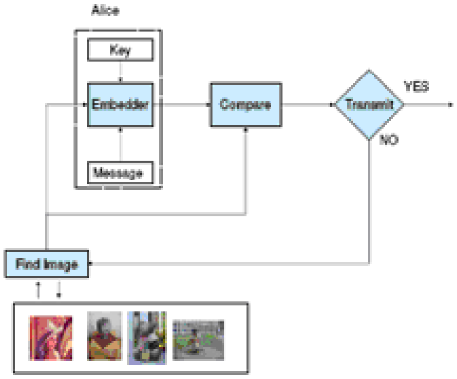

Figure 3. Cover Image Selection

There are two types of methods in digital images for hiding the message in cover image.

1. LSB (Least Significant Bit): This is method for embedding 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 [4].

2. MSB (Most Significant Bit): This method considers the value of the MSB of the pixels of the image for data hiding. The MSB bits of each pixels of an image are changed to a bit of a secret message that is to be hidden.

IV. Methods Of Steganography

- One Bit Stego
  In this method when images are used as the carrier in Steganography they are manipulated by changing one or more of the bits of the byte that make up the pixels of an image. This is the most secure method compared to the other methods discussed below.
- Two Bits Stego
  In this method two LSBs of one of the colors in the RGB value of the pixels will be used to store message bits in the image.
- Three Bits Stego
  In this method three LSBs of one of the colors in the RGB value of the pixels will be used to store message bits.
- Four Bits Stego
  In this method four LSBs one of the colors in the RGB value of the pixels will be used to store message bits.
- Color Cycle Stego
  In order to make the detection of the hidden data more difficult it was decided to cycle through the color values in each of the pixels.

V. LSB BASED DATA HIDING METHOD

LSB based technique is simple approach in which message bits are embed in the least significant bits of cover image [5].In this technique, the least significant bit of cover image is used to hide the secret message.

A).Algorithm for Least Significant Bit (LSB) method

Algorithm to embed text message using Grayscale Image is

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert the text message to binary
Step 3: Calculate LSB of each pixels 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 & convert each 8 bit into character

Algorithm to embed text message using color Image is

Step 1: Read the pixels of a given image and store in an array called image-array.
Step 2: Convert the message that is to be embedded into binary message.
Step 3: Read this binary message into an array called message-array
Step 4: Choose the pixel from the image-array and pick the characters from the message-array and place it in the LSB of pixel.
Step 5: Obtained image will be stego image that contains hidden data.

B .LSB Insertion

The most technique used today is LSB Insertion. The least significant bits of the cover-image are altered so they form the embedded information. Even LSB insertion is easy to implement, it is easily attacked.

Slight changes in the color palette and simple image manipulations will destroy the entire hidden information [7].

C. Evaluation of LSB methods on GIF file format

GIF file format is used for storing multiple bitmap images in single file. It was designed to allow easy interchange and viewing of image data stored on local or remote computer systems.GIF files are read as continuous stream of data and the screen is read pixel by pixel.GIF is a lossless compression format [3].

Three evaluation methods are,

1. Pattern analysis of Image Pixels

This method is based on looking for patterns in the bits that make up the pixel colors.

2. Pattern analysis of Image Palette

This method is based on looking for patterns in the images palette.

3. Low level Visual Inspection of Image Pixels

This method is based on carrying out a detailed inspection of selected sections of an image at a high degree of magnification.

D. Evaluation of LSB method in PNG file format

PNG (Portable Network Graphics) image file format is used for hiding messages. This is used as a container file.PNG supports indexed colors, gray-scale, and RGB. It works better in online viewing applications such as World Wide Web[10].

A PNG file starts with an 8-byte signature. The hexadecimal byte values are 89 50 4E 47 0D 0A 1A 0A.After the PNG header chunks will arise continuously.

A chunk will contains four parts: length, chunk type/name, chunk data and CRC. PNG images can use either palette-indexed color or made up of one or more channels. Since multiple channels can after a single pixel, the number of bits per pixel is often higher than the number of bits per channel. The file header of PNG is shown in Table 2

Table .2.File Header of PNG

Bytes	Purpose
89	Has the high bit set to detect transmission systems that do not support 8 bit data and to reduce the chance that a text file is mistakenly interpreted as a PNG, or vice versa.
50 4E 47	In ASCII, the letters PNG, allowing a person to identify the format easily if it is viewed in a text editor.
0D 0A	A DOS-style line ending (CRLF) to detect DOS-Unix line ending conversion of the data.
1A	A byte that stops display of the file under DOS when the command type has been used—the end-of-file character.
0A	A Unix-style line ending (LF) to detect Unix-DOS line ending conversion.

Table.3.Chunks within the PNG file

Length	Chunk Type	Chunk data	CRC
4 bytes	4 bytes	Length bytes	4 bytes

VI. Conclusion

Cryptography deals with taking a message and making it appear as random noise, unreadable to an outside world. It does nothing to hide the presence of message to itself. Steganography is the art and science of covering information in such a way that its presence is unnoticed. This paper discusses the LSB method to hide the secret message in the Least Significant bit of the image. The LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded.LSB method is applied for various file formats. This method can use for both GIF and PNG file format. 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.

Acknowledgement

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

References

[1] Ravi Kumar, Kavita Choudhary, Nishant Dubey, "An Introduction of Image Steganographic Techniques and Comparison", International Journal of Electronics and Computer Science Engineering.

[2] 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, pp.788-799.

[3] 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, September 2010 , pp .1-4.

[4] Dr. Ekta Walia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography, Global Journal of Computer Science and Technology", Vol.10, Issue 1, April 2010, pp.4-8.

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

[6] DeepeshRawat,VijayaBhandari,"Steganography Technique for Hiding Text Information in Color Image using Improved LSB Method", International Journal of Computer Applications,Vol.67, No.1, April 2013, pp.22-25.

[7] 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, 2009.

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

[9] M.Sivaram B.DurgaDevi J.Anne Steffi, "Steganography of two lsb bits", International Journal of Communications and Engineering, Vol.1– No.1, Issue: 01, March 2012.

[10] WaiWaiZin,"Message Embedding In PNG File Using LSB Steganographic Technique", International Journal of Science and Research (IJSR) Vol. 2 Issue 1, January 2013, pp. 227-230.