ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

Applications of Steganography in Information Hiding

[I]Deepak Garg, [II]Gourav Sharma
[I]M. Tech Student, M.M U. Mullana
[II]Associate Prof., M.M U. Mullana

Abstract
The fast development in the transfer of data through internet made it easier to transfer data precise and faster to the receiver. Security of information is one the significant factors of information technology and communication. Steganography is art and science of invisible communication. Steganography is the method in which the existence of the message can be kept secret. This is done through hiding information in other information, thus hiding the existence of actual information. In this paper we have provided a review on information hiding using steganography.

Keywords
Steganography; Least Significant Bit; Discrete Wavelet Transform; Cryptography etc.

I. Introduction

In today's world, the communication is the basic necessity of every growing area. Everyone wants their communicating data to be secret and safe [3]. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. In order to share the information in a concealed manner two techniques could be used. The possible two techniques are the following:
Cryptography
Steganography

A. Cryptography

It is a technique for securing the confidentiality of communication. Many different encryption and decryption methods have been implemented to maintain the secrecy of the message, it may also be necessary to keep the existence of the message secret.

B. Steganography

It is the art and the science of indistinguishable communication of messages. It is done by hiding information in other information, i.e. hiding the existence of the communicated information. In image steganography the information is hidden in images. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Hiding information into a media requires following elements [1]:

- The cover media (*C*) that holds the hidden data
- The secret message (*M*), may be plain text, cipher text or any type of data.
- The stego function (*Fe)* and its inverse (*Fe-1*).
- An optional stego-key (*K*) or password may be used to hide and unhide the message.

II. Methods of Concealing Datain Digital Image

Steganography is used for covert communication. The secret image which is communicated to the destination is embedded into the cover image to derive the stego image.

A. Least Significant Bit Substitution Technique (LSB)

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bitgrayscale bitmap image where each pixel is stored as a byte representing a gray scale value [5]. Suppose the first eight pixels of the original image have the following gray scale values [5]:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new grayscale values:

11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011

B. Discrete Cosine Transform Technique (DCT)

DCT coefficients are used for JPEG image compression [5]. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

C. Discrete Wavelet Transform Technique (DWT) [5]

The frequency domain transform we applied in this research is Haar-DWT, the simplest DWT [5]. A 2-dimensional Haar-DWT consists of two operations:
One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:
Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 1. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

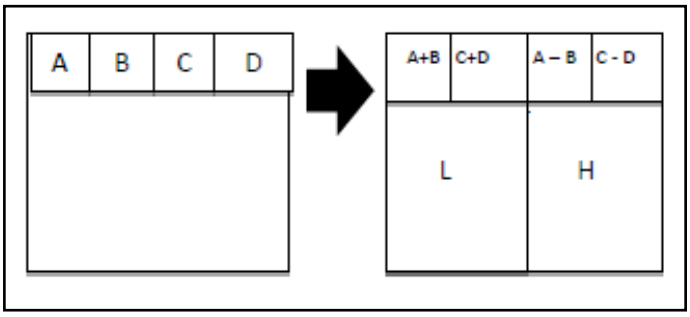

Fig. 1: The Horizontal Operation on First Row [5]

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Figure 2. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. The whole procedure described is called the first-order 2-D Haar-DWT.

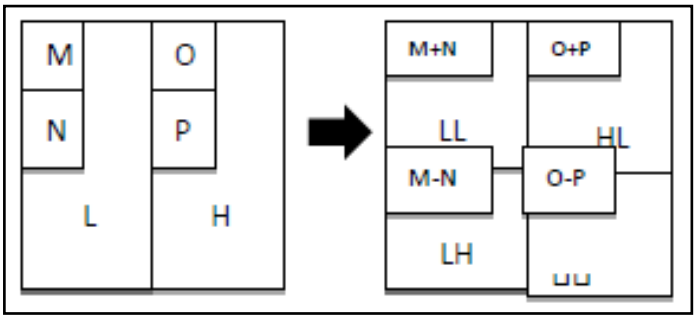

Fig. 2 : The vertical operation [5]

III. Steganalysis

Steganalysis is the process of identifying steganography by inspecting various parameter of a stego media. The primary step of this process is to identify a suspected stego media. After that steganalysis process determines whether that media contains hidden message or not and then try to recover the message from it [1, 6].

A. Steganalysis Techniques

The properties of electronic media are being changed after hiding any object into that. This can result in the form of degradation in terms of quality or unusual characteristics of the media: Steganalysis techniques based on unusual pattern in the media or Visual Detection of the same [1].

In the case of Visual detection steganalysis technique a set of stego images are compared with original cover images and note the visible difference. Signature of the hidden message can be derived by comparing numerous images. Cropping or padding of image also is a visual clue of hidden message because some stego tool is cropping or padding blank spaces to fit the stego image into fixed size. Difference in file size between cover image and stego images, increase or decrease of unique colors in stego images can also be used in the Visual Detection steganalysis technique.

IV. Various Steganographic Attacks

The steganographic attacks consist of detecting, extracting and destroying hidden object of the stego media. Steganography attack is followed by steganalysis [1]. There are several types of attacks based on the information available for analysis. Some of them are as follows: -

A. Known Carrier Attack

In this attack, the original cover media and stego media both are available for analysis.

B. Steganography Only Attack

In this type of attacks, only stego media is available for analysis.

C. Known Message Attack

The hidden message is known in this case.

D. Known Steganography Attack

The cover media, stego media as well as the steganography tool or algorithm, are known [1].

V. Evaluation of Image Quality

For comparing the stego image with cover results it requires a measure of image quality and the commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capacity [2].

A. Mean-Squared Error

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

$$MSE = \sum[I1(m,n) - I2(M,N)]^2 \div M * N$$

In the above formula M and N are the number of rows and columns in a input images, respectively.

B. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) will help to avoid this problem by scaling the MSE according to the given image.

$$PSNR = 10\log10\ (256^2 \div MSE)$$

PSNR is measured in decibels (dB) and it is a good measure for comparing restoration results for the same image.

C. Capacity

It is the size of the data in a cover image. The capacity can be modified without deteriorating the integrity of the cover image. In addition to the cover image perceptual quality a steganography embedding operation needs to preserve the statistical properties of the cover image and therefore capacity depends on the total number of bits per pixel and the number of bits embedded in each pixel of the image. Capacity is represented by bits per pixel (bpp). The Maximum Hiding Capacity (MHC) is represented by terms of percentage [2].

VI. Applications of Steganography

I. Confidential Communication and Secret Data Storing
II. Protection of Data Alteration
III. Access Control System for Digital Content Distribution
IV. E-Commerce
V. Media
VI. Database Systems.
VII. Digital watermarking [3].

ISSN : 2394-2975 (Online)
ISSN : 2394-6814 (Print)

VII. Steganography Softwares

Existing LSB Base Software is one of the popular and oldest techniques used to hide message in digital image is to hide it in the least significant bit (LSB) of pixel value. Some of the software are given below-

a. Mandelsteg by Henry Hastur
b. Steg by the JPEG group
c. S-tool by Andrew Brown
d. Gzip by Andrew Brown
e. Hide seek by Colin Maroney
f. Wbstego by Werner bailer
g. Enhanced LSB method

VIII. Conclusion

The network security is becoming more & more important as the number of data being exchanged on the Internet increases. Steganography and steganalysis are the important topics in information hiding. Steganography is the ability and discipline of writing hidden messages in such a way that no one, apart from the sender and projected recipient, suspects the existence of the message.

References

[1] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay and Sugata Sanyal "Steganography and Steganalysis: Different Approaches" arXiv preprint arXiv:1111.3758. 2011/11/16.

[2] Vanitha, Anjalin D Souza , Rashmi , Sweeta DSouza "A Review on Steganography – Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm" , International Journal of Innovative Research in Computer and Communication Engineering. Vol.2, Special Issue 5, October 2014, pp 89-95.

[3] Jasleen Kour and Deepankar Verma Steganography Techniques –A Review Paper International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-5)May 2014, pp 132-135.

[4] R.Poornima and R.J.Iswarya An Overview Of Digital Image Steganography International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013, pp 23-31.

[5] Stuti Goel, Arun Rana & Manpreet Kaur. A Review of Comparison Techniques of Image Steganography. Global Journal of Computer Science and Technology Graphics & Vision ,Volume 13, Issue 4,Version 1.0 ,Year 2013.

[6] E Lin, E Delp "A Review of Data Hiding in Digital Images" Video and Image Processing Laboratory (VIPER) School of Electrical and Computer Engineering Purdue University West Lafayette, Indiana.

[7] Rashi Singh and Gaurav Chawla A Review on Image Steganography. International Journal of Advanced Research in Computer Science and Software Engineering.Volume 4, Issue 5, May 2014, ISSN: 2277 128X.pp 686-689.