ISSN 2229-5518

Comparative Study of Image Stegnographic Techniques

Shilpa Saharan and Archana Toky[1]
Government College of Woman, Hisar-125001 (INDIA)

Abstract— Stenography is the method of communicating useful information in such a manner that no one can not even think that there is some transference of information. The message is not attracted by eavesdroppers and attackers because the observer cannot even detect the presence of message. For hiding the information, the most popular format is digital image. In this paper, we are doing comparative study of different stegnographic techniques. These techniques are analysed according to their ability of how much information they can hide and their robustness to different attackers.

Introduction

Security of confidential information is always remaining an issue. This led to the development of stegnographic techniques. The word stegnography is derived from the Greek words "stegos" meaning "cover" and "grabia" meaning "writing" [1]. It differs from cryptography. Cryptography encodes the data in such a way that third party cannot understand the meaning of message but in stegnographic approach, stegnographer try to avoid the existence of message from unintended recipient. Images are considered as the most popular file format that is used in stegnography. It is used because we can access the pixel of image and the hidden information cannot be noticed by the human eye. Images are divided into three types: binary (Black-White), grey scale and Red-Green-Blue (RGB) images. The binary image has one bit value per pixel represent by 0 for black and 1 for white pixel. While the grey scale image has 8 bits value per pixel represent from 00000000 for black and 11111111 for white pixel [2]. The RGB image is the most suitable because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution that does not affect image quality and make the message more secure. The principle behind the stegnography is that the secret message is hided inside the cover image by the hiding algorithm and sent to the receiver. The receiver applies the reverse process and reveals the data. The changes that are taken place in images are not noticed by human eye.

Image Stegnography techniques

Image steganography techniques can be divided into two broad categories: spatial domain based stegnography and Transform domain based steganography.

A Spatial Domain Method

In Spatial domain method, secret message is directly embedded in the image. The most common and simple method is the least significant bits (LSB) insertion method.

a) Least Significant bit

It replaces the last bit of some or all pixel of the image to the message that is to be hidden. If we are using 24-bit image, a bit of each of red, green and blue color components can be used. Suppose first 3 pixels of the image has the following values

(00101101 01010011 11011011)
(10111110 10000100 01001100)
(11010010 1 0101101 01100111)

To hide letter c, whose binary value is 10000011, we replace each last bit of each of the Red, Green and Blue of the pixel

(00101101 01010010 11011010)
(10111110 10000100 01001100)
(11010011 10101101 01100111)

Only 8 bits are changed. On average, only half of the bits of an image need to be modified to hide a Secret message. These changes cannot be perceived by human eye.

b) Hiding Image in Image using Block Method

The image is divided into blocks of equal size. Each block is equal to the size of the embedding image. Best pixel is selected to embed in the cover image. Best pixel is the pixel that gives minimum difference between it and the pixel to embed [3]. Suppose if pixel (i, j) to embed has a value 155, and corresponding pixel values are: 159, 160, 250, 230, 149, 148, 145, and 144. Then the pixel with value 149 will be selected.

c) Transform Domain Method

The Image is transformed and then message is embedded in image. The cover image is transformed from spatial domain t frequency domain. Discrete Cosine transformation is applied and then quantization of the DCT coefficients of the image.

a) JPEG stegnography

Initially, it was believed that steganography could not be used with JPEG images due to lossy compression. If an image is to compress into JPEG format, The RGB color space is first turned into YUV representation. Then image is transformed. For JPEG images, the discrete cosine transform(DCT) is used. With DCT transformation, a signal is transformed from the representation of an image to frequency domain, this is done by dividing the Image into 16*16 pixels block instead of 8*8 pixels block to improve the hiding

capacity. 16*16 quantization is taken. For embedding middle frequency coefficients for data are used because high frequency coefficients are discarded due to quantization process and lower frequency coefficient cause quality degradation of images.

The image is divided into blocks of 16*16 pixels and then DCT is used to transform each block into DCT coefficients. The DCT coefficients are scaled by 16*16 quantization table. The quantized DCT coefficient of each block are rounded to the nearest integers and then set in zigzag scan order. The least 2 significant bits of each middle frequency coefficient in the quantized DCT blocks are modified to embed 2 secret bits. JPEG entropy coding is applied to compress these resultant blocks and then JPEG files are obtained.

b) Wavelet transform technique

Wavelet transform converts spatial domain information to the frequency domain information. It represents a time frequency representation. It divides the high frequency and low frequency information on a pixel by pixel basis. DWT with the first level is used to decompose both secret and cover images, where each is broken into disjoint(4*4) blocks. Then a comparison is made between the blocks of the secret image and the cover blocks to determine the best match. It embeds information in the edge where human eye is less sensitive.

4) Spread spectrum Technique:

Spread spectrum is a form of Radio Frequency communication. It is when employed with stegnography, deals with cover image as noise because it appears as noise so difficult to detect. The cover is divided into sub images. When these subcover images are tiles, the technique is referred to as direct sequence spread spectrum stegnography. When the subcover images consist of separate points distributed over the cover image, the technique is referred to as frequency-hopping spread spectrum stegnography. The message is embedded in noise and then combined with cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of cover image, the embedded image is not perceptible to the human eye [5].

Evaluation of different techniques

There are several parameters to measure the performance of the stegnographic system

a) Undetectability: It represents the ability to avoid detection. Best steganographic techniques should neither be detectable by human eye nor by statistical attacks.

b) Robustness: It measures the ability of the stegnographic technique to survive the attempts of removing the hidden information. Such attempts include image manipulation, data compression and image filtering.

c) Payload capacity: It is the third parameter that represents the maximum amount of information that can be hidden and retrieved successfully.

Table1: comparison of Image Steganogrpahy techniques

	LSB	JPEG	Wavelet	Spread Spectrum
Undectectability	High	High	High	High
Payload capacity	Low	Low	High	High
Robustness	High	High	Medium	Medium

conclusion

This paper reviewed the main stegnographic techniques. There exist a large number of techniques to hide the information in images. All the techniques have advantage and disadvantage both. If one technique lacks in robustness, its payload capacity is better. For example, the spatial domain approaches are considered not to be robust against lossy compression. Transform domain techniques are more robust for lossy compression image formats, but this advantage is achieved at the cost of payload capacity. Thus to decide that which stegnographic algorithm to use, he would have to decide which application he want to use.

` **References**

[1]T.Sharp, "An implementation of key-based digital signal steganography", in Proc. Information Hiding Workshop, Springer LNCS, pp. 13-26, 2001

[2] Atallah M. A1. Shatnawn, A New Method in image Stegnography with improved Image Quality, Applied Mathematical Sciences, Vol 6, 2012, no. 79, 3907-3915.

[3] Kanzariya Nitin K., NimavatAshish v., comparison of various Images stegnography Techniques, International Journal of computer science and management Research vol 2 Issue 1 January 2013.

[4] Adel Almohammad, GheorghitaGhinea, Robert M. Hierons, "JPEG steganography: a performance evaluation of quantization tables, International conference on Advanced Information Networking and Applications (2009)

[5] Image Steganography Techniques. An overview, Nagham Hamid, AbidYahya, R. Badlishah Ahmad & Osamah M.AI-Quershi, International Journal of computer Science and Security(IJCSS), Volume(6): Issue(3):2012

[6] Mohammad Shiali-Shahreza, "A new method for real time steganography", ICSP 2006 Proceedings of IEEE.

[7] A.Almohammad, R.M.Hierons and G.Ghinea,"High Capacity Steganographic Method Based Upon JPEG", The Third International Conference on Availability, Reliability and Security. ARES08, Barcelona, Spain, 4-7 March, 2008, pp. 544-549.

[8]Jagvinder Kaur and Sanjeev Kumar," Study and Analysis of Various Image Steganography Techniques" IJCST Vol. 2, Issue 3, September 2011.