Steganography In Image: A Review

Sarabjot Singh Grewal[1], Priya[2]
[1]Department of Electronics and Communication Engineering, Punjabi University, Patiala, India
[2]Department of Electronics and Communication Engineering, Punjabi University, Patiala, India
[1]sarab.grewal001@yahoo.com
[2]priyasharma0693@gmail.com

***Abstract:* These days while sending a data over an unsecure channel, the most important thing is security. To acquire that security of data techniques such as data hiding plays an important role. Steganography is a science to hide data in such a way that the hidden information is not detectable. Different carrier file formats can be used to hide the data like, images, videos, audios, text. But the most popular one are the digital images due to their high frequency on internet. Now there are several steganography techniques to hide data inside images. Different applications require different steganography techniques. This paper intends to look at different image Steganography Techniques. Also take a look at which steganography technique is more suitable for which applications.**

Keywords: **Steganography, Spatial Domain, LSB, Transform Domain, Spread Spectrum.**

I. INTRODUCTION

Steganography is the science of hiding a file, message, image, or video within another file, message, image, or video. The word steganography is derived from a Greek words steganos meaning "covered, concealed, or protected", and graphein meaning "writing".

The advantage of steganography over cryptography is that the secret message does not attract attention to itself. In cryptography the encrypted messages, no matter how unbreakable, arouse suspiciousness. Therefore, whereas cryptography is the practice which only protecting the contents of a message, steganography is concerned with the fact that a secret message is being sent, as well as is secure over its path and is not detected to be present in the cover.[7]

The Steganography techniques have a wide range of applications. It is used in the department of defense for the transmission of secret data safely. Used in identification using smart identity cards. Stegnography is used in medical for imaging for the processes like Tomography etc. Another application is in industries like bottling industries. These days Steganography is used in colored printers, these printers do add a small yellow dot on every page, these dots secretly contain serial number of that printer.[7]

The history of steganography goes back to 440 B.C. Histiaeus use to have his most loyal servant as a messenger. He use to shave all the hair from his slave's head and then tattoo the message on his scalp. Now when the hair use to grow back the messanger would go to the destination and again shave his head to retrieve the message.[1]

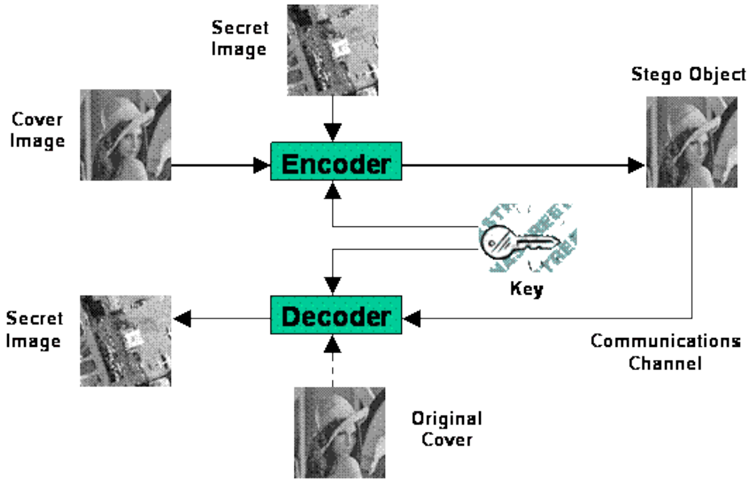

Fig.1. Basic Diagram Of Image Steganography[8]

The above diagram shows the basic process followed during Image Steganography. Here we have a cover image. It is an image that will work as a carrier to carry the message i.e. Secret Image to the receiver. The cover and secret image are combined using a key. The key is needed to be known to the receiver as well, so as to retrieve the secret image from the cover image.

II. IMAGE STEGANOGRAPHY TECHNIQUES

Image Steganography is classified into two categories: Spatial-domain based Steganography and the Transform domain based Steganography.

A. Spatial Domain Based Steganography

In spatial domain technique, the messages to be hidden are embedded directly in the cover image. Here, the most common and simple Image Steganography method LSB insertion method i.e. least significant bits insertion method is used. In LSB method, the least significant bits (LSB) of the pixels are replaced by the message bits which are permuted before embedding the secret message in the cover image.[6]

B. Least Significant Bit Technique

Least significant bit (LSB) Replacement is a common and a simple method of embedding information in a cover image. The least significant bit (8 number bit) of some of the bytes or all of the bytes inside an image are replaced with a bit of the hidden message. When we use a 24-bit image, a bit of each of the red, green and blue color can be used, since they are all represented by a byte. That means, one can store 3 bits in each pixel. In an image of 800 X 600 pixels, a total amount of 1, 440, 000 bits or 180, 000 bytes of embedded data can therefore be stored.[4]

Example, 3 pixels grid for of a 24-bit image can be as follows:

(00101101 00011100 11011101)

(10100111 11000101 00001101)

(11010010 10101101 01100011)

Now when the number 500, having a binary representation “11110100”, is embedded into the least significant bits of this part of the image. the resulting grid is as follows:

(00101101 00011101 11011101)

(10100111 11000100 00001101)

(11010010 10101100 01100011)

Here the number 500 was embedded into the first 8 bytes of the grid, from these only the 3 “BOLD” bits needed to be changed according to the message which was embedded. On average, only half of the bits in an image will be needed to be modified to hide a message using the maximum cover/carrier size. By changing the LSB of a pixel, it results in small changes in the intensity of the colors of the cover image. These changes cannot be identify by the human eye, thus the message is successfully hidden in image.

Fig.2. The Cover Image.[1]

Fig.3. The Stego Image.[1]

C. HIDING GRAY IMAGES USING BLOCKS TECHNIQUE

In Internet these days the security of the digital data being transmitted has becomes a greater issue. The Block technique helps to increase the security level of the hidden data i.e. the possibility of the detecting the hidden message is reduced. In this method a gray image is hidden inside another gray image. The cover image is divided into blocks of equal sizes, where each block size is equal to that size of the blocks of the embedding image. Now the pixels in the embedding image are compared with the pixels of the cover image. The pixel in the cover image having value closest to the value of the pixel in the cover image will be used to embed that specific pixel and so on. [2]

D. TRANSFORM DOMAIN METHOD

When a large amount of data is to be hidden with greater security then the Transform Domain Method is used. Here the information is hidden in the frequency domain and for that the magnitude of all of discrete cosine transforms (DCT) coefficients of cover image are altered. The 2-dimensional DCT transforms the image blocks from spatial domain to frequency domain. Then the cover image is divides into 8X8 block size and then DCT is applied on each block of the cover image.[3]

E. JPEG IMAGE STEGANOGRAPHY TECHNIQUE

Earlier it was assumed that the JPEG image cannot be used to hide data in them i.e. the Steganography is not possible using the JPEG images. This is because JPEG images use lossy Compressions due to which parts of the data inside the image are being altered. The data is hidden in the redundant bits when using the Steganography technique and the problem with the JPEG images is that the redundant bits are left out due to which there is a danger of damaging the hidden data. Therefore it is not possible to hide or embed some data inside an image that is using lossy compressions. So, the JPEG compression algorithm is divided into stages i.e. Lossy Stage and Lossless Stage. These stages are quantization and the DCT phase. The Huffman coding is used in lossless to further compress the data. By using the LSB insertion method the message to be hidden can be embedded into the least significant bits of the coefficients and then the Huffman encoding can be applied.[4]

F. SPREAD SPECTRUM IMAGE STEGANOGRAPHY TECHNIQUE

In Spread Spectrum Image Steganography Technique the cover signal used is Digital Imagery. The information bits are hidden within the digital images by using Spread Spectrum, hence not allowing the detection of the hidden data. The error probability is too low as error control coding is used here. Here the original image is not required to extract the hidden data. A key is needed to be processed at the receiver end to get the hidden information. The detection of the hidden data is not detectable by human eye or computer. At low level of compressions this method provides noiseless transmission.

III. CONCLUSION

Some of the Image Steganography techniques were discussed in this paper, although there are a large number of data hiding techniques that exist. Different types of data hiding techniques are used to hide data in different types of image formats and they all have their own week and strong points. Some lack in data capacity, some in security and some in robustness. The least Significant Bit technique in BMP and GIF images has both data capacity and robustness but there is a chance of detection of hidden information in the image. Before deciding the Steganography Technique and algorithm to be used to hide an information one has to first decide the application he is using this algorithm for. One has to compromise for one factor to get good results for other factors.

REFERENCES

[1] Mr. Falesh M. Shelke1, Miss. Ashwini A. Dongre2, Mr. Pravin D. Soni “Comparison of different techniques for Steganography in images”. International Journal of Application or Innovation in Engineering & Management (IJAIEM) Feb2014.

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

[3] Blossom kaur1, Amandeep kaur2 and Jasdeep singh, ”Steganographic approach for hiding image in dct domain” International Journal of Advances in Engineering & Technology, July 2011.

[4] Dumitrescu, S., W. Xiaolin and Z. Wang, 2003. Detection of LSB steganography via sample pair analysis. In: LNCS, Vol. 2578, Springer-Verlag, New York, pp: 355 -372.

[5] Jarno Mielikainen, "LSB Matching Revisited", Signal Processing Letters, IEEE, Publication Date: May 2006 Volume : 13, Issue : 5, pp. 285- 287.

[6] Johnson, N.F and Jajodia, S., “Exploring Steganography:Seeing the Unseen”, Computer Journal, February 2008.

[7] https://en.wikipedia.org/wiki/Steganography

[8] Jonathan Cummins, Patrick Diskin, Samuel Lau, Robert Parlett, and Mark Ryan School of Computer Science, The University of Birmingham. “Steganography and Digital Watermarking”.2004.

[9] M.J.Thenmozhi1, Dr.T.Menakadevi2 “ A New Secure Image Steganography Using Lsb And Spiht Based Compression Method” International Journal of Engineering Research & Science (IJOER) March- 2016.

[10] Dr. Rajkumar L Biradar1 , Ambika Umashetty2 “A Survey Paper on Steganography Techniques” International Journal of Innovative Research in Computer and Communication Engineering January 2016.