International Journal of Emerging Engineering Research and Technology
Volume. 2, Issue 2, May 2014, PP 30-36

Comparative Study of Various Steganography Techniques

Ekta Dagar, Sunny Dagar,
Department of Computer Science and Engineering,
Manav Rachna College of Engineering,
Faridabad, India

Abstract: *Due to the high growth in the field of Computer Networks and Internet, there is a need for a secure transfer of information over the network. The data is in a great threat to be hacked by the hackers as it is transferred over the communication channels. Image Steganography is a technique which hides secret information inside an image and conceals the existence of the communication. No one could identify whether any communication is going over the network. In recent years, many steganography techniques have been developed. This paper presents a comparative study on some of the existing steganography techniques. The PSNR value is used to measure the quality of stego images. Larger PSNR value indicates better quality of image or lower distortion.*

Keywords: *Image Steganography, LSB, Information Hiding, cover image, stego image, PSNR*

1. INTRODUCTION

The Internet has become the most important source of information in today's life which offers the users to exchange information. But the transfer of such information leads to a great security threat. Steganography is the technique of hiding confidential information to conceal the existence of the embedded information. It is the art and science of invisible communication. It hides the secret information inside other information (cover image in this case), thus preventing the presence of secret information inside communicated information (the cover image which is sent to the receiver). The word steganography is derived from the Greek words "steganos" meaning "cover" and "graphei" meaning "writing" [2] defining it as "covered writing". Steganalysis is the art and science of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography.

Steganography has come from ancient History. In Histories, the Greek Historian Herodotus writes of a nobleman, Histaeus, wanted to communicate with his son-in-law in Greece. So, for the communication to be secret, he shaved the head of one of his most trusted slaves and tattooed the message on his scalp. After some days, when slave's hair grew back, he was dispatched with the message. In the Second world war, Germans developed a Microdot technique in which the information especially photographs were reduced in size which was difficult to detect when it was sent over an insecure channel within a normal cover message. Another form of Invisible writing is through the use of Invisible inks. In the world war-II, a normal letter may contain a different message written with such invisible inks. Common sources of Invisible inks were milk, vinegar and fruit juices which get darkened when heated.

Generally steganography is confused with cryptography because both techniques are used to protect information. The difference between these two is that the former focuses on keeping the existence of a message secret whereas the latter focuses on keeping the contents of a message secret [4]. In Cryptography, the comparison is done between the plaintext and the cipher text whereas in steganography, the comparison is made between the cover image and the stego image.

The steganography generally comprises of the following:

-a cover image/object, key, message to be hidden for embedding

-a stego image/object, key for extraction of hidden message

A cover image is the image which is used as a cover for the message to hide and a stego image is the image which is formed by the combination of normal image and secret message.

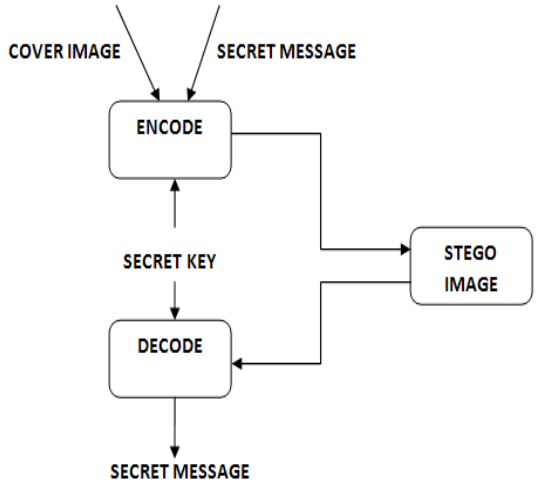

Figure 1. *Steganography operation*

There are different kinds of Steganography:

- Text
- Image
- Audio/Video
- Protocol

One of the most important methods of Steganography for hiding the information is in the Text. It hides the secret message in every n^{th} letter of every word of a text message. Images are the most usable cover objects for steganography. Different techniques for images will be discussed later in the sections. Audio steganography works along with masking which exploits the properties of human ear to hide information without being noticed. A small, but audible sound becomes inaudible in the presence of other louder audible sounds [2]. Protocol steganography refers to the process of hiding the secret message behind the network packets used in network transmission. There are covert channels exists in the layers of OSI model where steganography can be used.

In Image steganography, the information is hidden exclusively in images. Images are the basic cover objects used for steganography. The digital color images are the collection of pixels which usually stored in 24 bit files and uses RGB color model with each primary color representing 8 bits each. By varying the intensity of the RGB values, a finite set of colors spanning the full visible spectrum can be created [3].

2. Related Work

Many efficient image steganography algorithms have been proposed till date but still there is a lot of space for research in this vast and growing field.

- Arvind Kumar, Km. Pooja [1] presented paper on Image steganography-A Data Hiding Technique and discusses about how digital images can be used as a carrier to hide messages. It combines the secret image within the carrier image and that hidden image is difficult to detect without its retrieval. This paper also analyses the performance of some steganography tool.
- S.M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain [7] presented paper on a more efficient approach on Image Steganography, which is based on Least Significant Bit substitution to improve the security level of hidden information. It is an approach of substituting LSB of RGB true color image. In this paper, hidden information is stored into different position of LSB of image depending on the secret key and calculates the Peak Signal-to-Noise ratio.
- Rosziati Ibrahim, Teo Suk Kuan [6] proposed an Algorithm to hide data inside an image using Steganography technique. The proposed algorithm uses Binary codes

and pixels inside an image. By applying the proposed algorithm, a system called Steganography Imaging System is developed. Various sizes of data are stored inside the images and a PSNR value is calculated for each of the images tested.

- R. Chandramouli, Nasir Memon [3] presented a paper on the analysis of LSB Based Image Steganography Techniques in which some specific Image based Steganography techniques are undertaken which shows that an observer can indeed distinguish between images carrying hidden messages and images which do not carry a message and hence derives a closed form expression of the probability of detection of the images. It then identifies as how many bits can be embedded in order to protect the hidden image. A prisoner's problem is undertaken in the paper in which Alice and Bob are two persons who wish to communicate with each other in order to discuss an escape plan. However all communication between them is examined by a warden.
- Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar [8] presented a paper on An Image SteganographyTechnique using X-Box Mapping. This paper represents a LSB technique in spatial domain using X-Box mapping where four X-Boxes with sixteen different values are used which are mapped to the four LSB's of the image.
- K. Pramitha, Dr. L.Padma Suresh, K.L.Shunmuganathan, "Image Steganography using MOD-4 Embedding Algorithm based on Image contrast". In this paper [9], a new image steganography method based on image contrast is presented. A 2*2 valid block is selected to embed the secret message and a modulo-4 arithmetic operation is applied to the blocks to embed a pair of binary bits using the shortest route modification scheme. Every secret key is encrypted using RSA Encryption algorithm and data is embedded inside the image using pixels. The method is also tested on different grey scale images and provides larger embedding capacity being less detectable by steganalysis method.
- Anderson, R.J. & Petitcolas, F.A.P. [5], "On the limits of steganography" have proposed a LSB based algorithm in which the quality of the retrieved image is poor.
- Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena [10] presented a paper on Security Improvisation in Image Steganography using DES. Their proposed work presents an image steganography technique based on Data Encryption Standard (DES) using the strength of S-Box Mapping and a secret key. The preprocessing of secret data changes the intensity of pixels which provides a high level of security to the encryption algorithm.

3. TECHNIQUES OF STEGANOGRAPHY

Various Methods are used to hide information inside an Image. The most common methods are:

3.1 LSB Substitution

Least Significant Bit (LSB) Insertion/Substitution is one of the most widely used approaches to hide data in the images. It is a spatial domain technique in which the secret information is stored in image bits by replacing the actual bits of the image with the secret information bits and is then stored into the specific position of Least Significant Bit (LSB) of a cover image. An altered image with slight variations in its colors will be indistinguishable from the original image by a human eye.

Large Images are most desirable for this technique because they have enough space to hide the data in it. The best quality hidden message is normally produced by using a 24-bit bitmap as a cover image.

For example, suppose we want to hide data i.e. 01001010. Following are the three adjacent pixels (8 bytes):

Pixel 1	11000101	10010111 10010101
Pixel 2	10110011	10011100 10100100
Pixel 3	00001100	10010100 11001011

After hiding process, pixels would be:

Pixel 1	1100010<u>0</u>	10010111 1001010<u>0</u>
Pixel 2	1011001<u>0</u>	1001110<u>1</u> 10100100
Pixel 3	0000110<u>1</u>	10010100 11001011

In this way, the bits get substituted in the corresponding pixels. This is a very general approach and if the retrieval methods are known, one can easily extract the hidden information.

Another variation of the LSB would be randomization in which the secret message is spread out among the cover image in a random manner and a secret key is used for providing security. The secret key is shared only between the sender and receiver. The purpose of the key is to generate pseudorandom numbers, which will identify where and in what order the hidden message is laid out.

PSNR Calculation

A Peak Signal-to-Noise Ratio (PSNR) value is calculated to measures the quality of stego images. Larger PSNR value indicates better quality of image or lower distortion. PSNR is defined via the mean squared error (MSE) for two m*n monochrome images I and K where one of the image is considered a noisy approximation of the other. It is defined as [7]:

$$PSNR = 10.\log10 (MAX_I^2 / MSE)$$

$$= 20.\log10 (MAX_I / sqrt (MSE))$$

The Mean Squared Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two metrics used to compare the Image quality. The MSE represents the cumulative squared error between the stego and the original image. The distortion in the image can be measured using MSE. Lower the value of MSE, lower is the error. The MAX is the maximum possible pixel value of the images. For example, if the pixels are represented using 8 bits per sample, then the MAX value is 255.

If the value is larger among all other techniques, then it will results in the better quality of image.

3.2 Masking and Filtering

Masking refers to hide a signal by a different signal so that the first signal is not visible at all. Masking and filtering is mainly used for watermark techniques. It is based on the human visual ability which cannot detect slight changes. The data is embedded into the image and even if the image is manipulated by compression or cropping techniques, the data will not be lost.

Masking and filtering techniques are usually applied to 24-bit and grey-scale images. Watermarking techniques like visible watermarks are not actual steganography. But it extends the information and becomes an attribute of the cover image. Digital watermarking contains information like ownership, copyright, license etc. The object of communication here is the cover image.

Masking is more robust as compared to LSB Insertion technique in terms of image processing, cropping, image compression etc. It embeds the information by hiding it at the noise level in the cover image. Therefore, it is useful for the lossy JPEG Images. This method has a high degree of luminance to make the watermarks more secure and will not be detectable by the human eye.

3.3 Algorithm Transformation

In the transformation methods, two things are considered:

(i) To accommodate the data of the payload, there is slight modification in the coefficients and

(ii) The unused coefficients of the payload data are replaced.

Data can be embedded in the Transformation algorithms by changing the coefficients of transformation of an image into the cover image. In spatial domain, the images are compressed for image compression which may results in the loss of secret message information. To deal with this situation, data can be embedded in Frequency domain which applies the transformation to the image. There are various transformation techniques like discrete cosine transformation technique (DCT), Fast Fourier transformation technique (FFT), Discrete Wavelet transformation technique (DWT). The implementation technique is same for all the three but the main focus is on JPEG images which uses DCT for Compression.

DCT is a lossy compression transform in which the cosine values cannot be calculated exactly and repeated calculations using the limited precision is required. It transforms the cover

Image into a frequency representation by grouping the pixels into non-overlapping blocks of 8*8 pixels and then pixels blocks are transformed into 64 DCT coefficients each. The transformed cover image is then quantized and modified according to the secret message. It is then results in a high level of capacity and controls the compression ratio.

While doing Decompression, the resultant image goes through decoding, de-quantization, inverse DCT etc. Then the real valued pixels are obtained which are rounded to the nearest integers and are truncated to a finite range.

DWT domain based embedding technique actually operates on DCT or DFT. Embedding is done by modifying the least significant bits of the selected wavelet coefficients. FFT domain based embedding technique embeds the data through the Fourier transform mapping but it produces round-off errors, that is why the technique is not so useful for hidden communication.

But we cannot embed too much data in the frequency domain as it causes a loss of quality of the cover image.

4. Factors Affecting Steganography

There are certain factors which affect steganography. They are Capacity, Security, Robustness, Invisibility and Computational Complexity. Capacity refers to the total amount of data bits that can be embedded in the cover medium. Security is related to the ability of an eavesdropper to capture the hidden message. Robustness refers to the ability of a stego image to secure itself against scaling, filtering, noise and cropping. Invisibility is the strength of the stego image to be kept unnoticed by the human eye. Computational Complexity refers to the computational cost of embedding and extracting of the secret message.

5. Conclusion

This research describes a comparative study of some steganography techniques and the background of steganography. Steganography is a useful technique for Information Security. It is a powerful tool which enables people to communicate secretly over the Network. The purpose of this study is to identify some useful, reliable and efficient steganography techniques.

Table 1. *Comparison of the Techniques*

Technique	Description	Features	Limitations
LSB Substitution	Data hides at the least significant bits of the pixel.	Less chances of degradation of the original image with more hiding capacity.	The data may be lost while doing image manipulation (compression), less robust, simple attacks could destroy the hidden data.
Masking and Filtering	It masks secret message over the cover image by changing the luminance i.e. embedding the message within significant bits.	It is more robust as compared to LSB substitution. It is used for lossy JPEG images as it is resistant to image compression, processing, cropping etc.	It can be detected by simple statistical analysis and tools.
Algorithm Transformation	Data is embedded in cover image by changing the coefficients of transform of the image.	Compression is used to reduce bandwidth, hence it is achieved by using quantization techniques and run length coding of the transformed coefficients. It increases the level of capacity and controls the compression ratio.	Some of the transformation techniques like FFT (Fast Fourier Transform) generates round off errors which is unsuitable for hiding process. Hence, large amount of data cannot hide as it causes degradation in the cover image.

REFERENCES

[1] Arvind Kumar, Km. Pooja, "Steganography-A Data

[2] Hiding Technique", International Journal of Computer Applications, Vol.9-No.7, November 2010.

[3] T.Morkel, J.H.P. Eloff,M.S. Olivier, "An Overview of Image Steganography", ICSA Group, University of Pretoria,0002,Pretoria,South Africa

[4] R. Chandramouli, Nasir Memon,"Analysis of LSB Based Image Steganography Techniques", Computer Science Department, Brooklyn, NY 11201

[5] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[6] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[7] Rosziati Ibrahim and Teo Suk Kuan, "Steganography Algorithm to hide Secret Messages inside an Image" University Tun Hussein Onn Malaysia (UTHM), Batu Pahat 86400, Johor, Malaysia, February 25, 2011.

[8] S.M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", Khulna University, Khulna 9208,Bangladesh,proceedings of 14th International Conference on Computer and Information Technology(ICCIT 2011)22-24 Dec-2011.

[9] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, "An Image Steganography technique using X-Box Mapping",IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM-2012) March 30-31,2012

[10] K. Pramitha, Dr. L.Padma Suresh, K.L.Shunmuganathan, "Image Steganography Using MOD-4 Embedding

Algorithm based on Image Contrast", International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011), pg.364-369

[11] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, "Security Improvisation in Image Steganography using DES", IEEE, pg. 1094-1099.

[12] Ramanpreet Kaur, Baljit Singh, Ishpreet Singh, "A Comparative Study of Combination of Different Bit Positions in Image Steganography", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.5, Sep-Oct. 2012, pp-3835-3840.

AUTHOR'S BIOGRAPHY

Ekta Dagar, am pursuing M.tech from Manav Rachna College of Engineering.I completed my B.tech with 80% marks and distinction. I live in Faridabad, Haryana.

Sunny Dagar, am working as an Assistant Lecturer in Manav Rachna college of Engineering. I live in Najafgarh, Delhi. I wrote various research papers in which one paper "RGB based dual key image Steganography" is published in IEEE last year.