ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024

Survey on Image Steganography and its Techniques

Manish chaudhary[1], Kamaldeep Joshi[2], Rajkumar Yadav[3], Rainu Nandal[4]
[1]M.tech. Student, CSE Department, University Institute of Engineering and Technology,
M. D. University, Rohtak, Haryana, India
[1]Email: manishchaudhary2403@gmail.com
[2, 3, 4] Assistant Professor, CSE Department, University Institute of Engineering and Technology,
M. D. University, Rohtak, Haryana, India

***Abstract:* - In present Scenario of the world, Internet has almost reached to every aspect of our lives. Due to this, most of the information sharing and communication is carried out using web. With such rapid development of Internet technology, a big issue arises of unauthorized access to confidential data, which leads to utmost need of information security while transmission. Cryptography and Steganography are two of the popular techniques used for secure transmission. Steganography is more reliable over cryptography as it embeds secret data within some cover material. Unlike cryptography, Steganography is not for keeping message hidden from intruders but it does not allow anyone to know that hidden information even exist in communicated material, as the transmitted material looks like any normal message which seem to be of no use for intruders. Although, Steganography covers many types of covers to hide data like text, image, audio, video and protocols but recent developments focuses on Image Steganography due to its large data hiding capacity and difficult identification, also due to their greater scope and bulk sharing within social networks. A large number of techniques are available to hide secret data within digital images such as LSB, ISB, and MLSB etc. In this paper, a detailed review will be presented on Image Steganography and also different data hiding and security techniques using digital images with their scope and features.**

Keywords: - Steganography, Steganalysis, stego-key, stego-image, carrier-image, LSB, cryptography, factor, DCT, DFT, DWT, Spatial domain, Transform domain.

I. INTRODUCTION

The word “Steganography” is Greek originated word in which “steganos” means covered and hidden and “graphy” means writing [3]. This embedding technique, i.e. steganography, is a process of avoiding and eliminating the attention of intruders towards the ongoing confidential interaction.

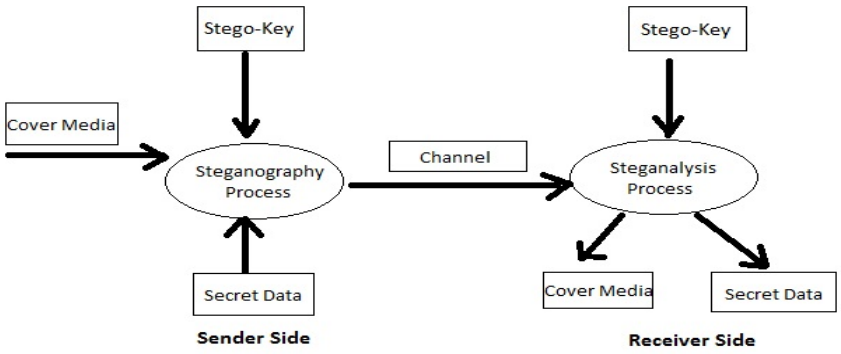

Figure.1. Steganography system

The check done over the communicated material to identify presence of covered message in the field of Steganography is known as Steganalysis.

It aims to conquer steganography process. Steganalysis is founded on the factuality that the carrier gets altered and an unusual signature or degradation is introduced whenever information is hidden within media. Hence steganography system has to assure that covered message is not detectable.

A. Image Steganography

A digital image is defined using grid points called pixels as a 2-Dimensional matrix of multiple colors. Gray images are formed of 8 bits and colored images are utilizing 24 bits to present their models, like RGB model [4]. When digital images are used as cover material than steganography process is specifically called as Image Steganography.

Figure.2. Cover image

Consider above Figure 2 as cover image, the secret message “This is an example showing implementation of Image Steganography and how the stego image looks like.” is embedded in it and transformed into stego-image given below in Figure 3, using some Image steganography technique. As we can see, it is almost impossible to detect any kind of alteration between two images with normal observation.

Figure.3. Stego-image

Image steganography process is carried out in two stages [7]:

(i) Creation of stego-image using secret message and cover image.

(ii) Extraction of hidden message from stego-image.

At sender’s side, secret message is hidden within cover image with an untold key plus an algorithm for embedding process. This untold key selects pseudo-random pixels to hide data [7].

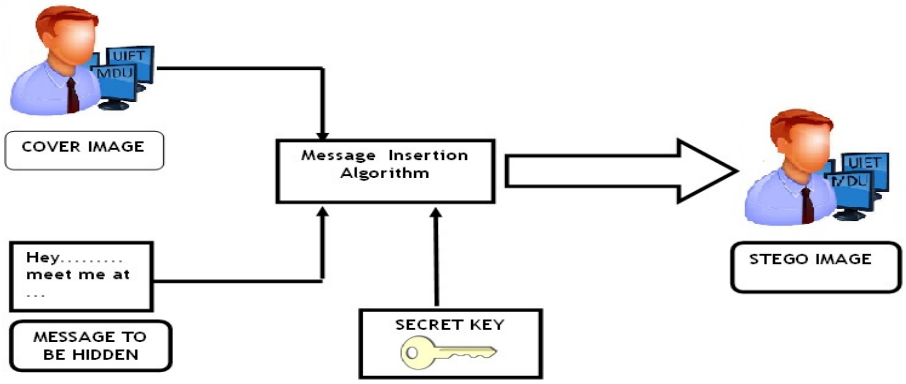

Figure.4. Message insertion at sender’s side

Secret key is shared amongst communicators. This key secures the data in case intruder gets to know about the stego-image and have embedding algorithm. Above Figure 4 shows steganography process at sender’s side.

At receiver’s side, secret message is obtained from stego-image using secret key and embedding algorithm. Below Figure 5 shows Steganalysis process at receiver’s side.

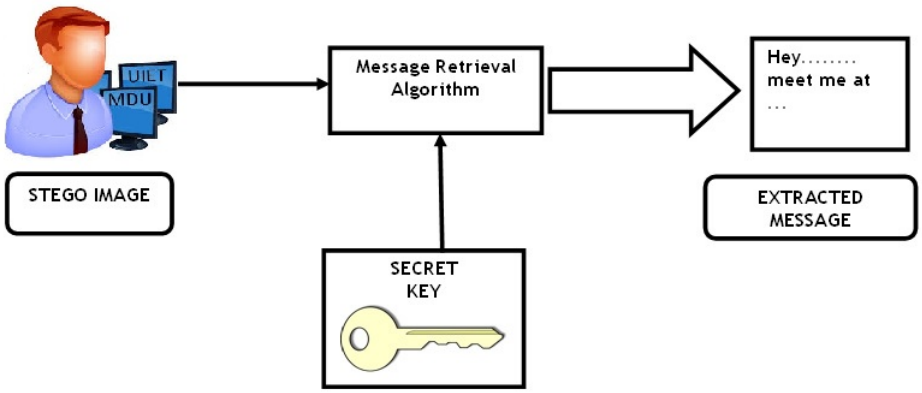

Figure.5. Message retrieval at receiver's side

B. Factors Effecting Steganographic Methods

By comparing stego-image with cover image, the effectiveness of stego- image can be judged. Given below are some factors that helps ensure how effective and robust any steganography technique is:

(i) Robustness: It is the ability of hidden data to stay intact within stego-image if it suffers from transformations, like rotation or scaling, noise exposure, blurring or sharpening, liner or non-linear filtrations, lossy compression, cropping etc [9].

(ii) Imperceptibility: Invisibility of steganography algorithm refers to imperceptibility. It is the foremost requirement of steganography. The stego- image must stay unnoticed to human-vision.

(iii) Payload Capacity: The measure of confidential information that could be inserted within carrier image is called payload capacity. It should be large enough for efficient embedding. While applying steganography, the statistical proportions and visionary quality of cover-image must sustain. So, payload capacity relays on number of bits in each pixel and also on count of bits encoded within every pixel.bpp (bits per pixel) and MHC (Maximum Hiding Capacity) shows capacity of medium in percentage [5].

(iv) MSE (Mean Squared Error): MSE is calculated by averaging the squared difference among distorted-image and cover-image. Equation for MSE is given below:

$$\text{MSE}= \frac{\sum(M,N)\ [I_1(m,n)-I_2(M,N)]\text{^}2}{M*N} \qquad [5]$$

The number of rows and columns within two images are given by M and N respectively. 'I_1' and 'I_2' are two images within whom pixels are compared. Higher value of MSE indicates dissimilarities between two images.

(v) PSNR (Peak Signal to Noise Ratio): PSNR is the ratio among powers of any signal to corrupting noise. This corruption due to noise damages the fidelity of its representation [7].

$$\text{PSNR}= 10 \log_{10} (256^2/ \text{MSE})$$

It is measured in decibels (dB). Higher the value of PNSR better will be the quality of stego-image.

(vi) SNR (Signal to Noise Ratio): It represents the ratio of Signal-to-Noise powers in the background of desired image.

(vii) NCC (Normalized Cross-Correlation): NCC is used to calculate and evaluate homogeneity (or non-homogeneity) amongst cover-image and stego-image. It is almost a concept of template matching that focuses on checking stego-image for discovering induced patterns due to embedding which makes it traceable for intruders. Its value ranges from -1 to 1.

II. IMAGE STEGANOGRAPHY TECHNIQUES

Image steganography is classified within two basic types of embedding schemes (as shown in Figure 6): spatial domain and transform domain embedding schemes.

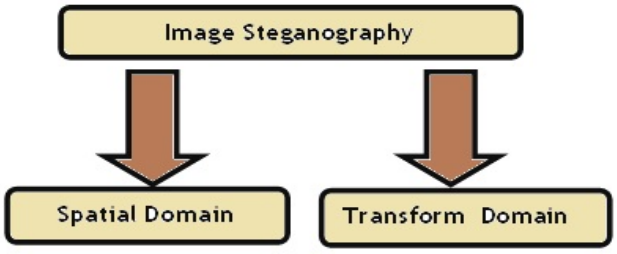

Figure.6. Classifying image steganography

In spatial domain scheme, the secret message is directly embedded in cover image and this information is embedded in the intensity of pixels of image [7]. In this scheme, secret message is embedded in redundant and less significant parts of the cover image. LSB is most commonly used spatial technique.

In transform scheme, the confidential data is settled within frequency-domain of already transformed cover-image. Here, in transform scheme, secret message gets embedded in significant parts of cover image. Hence this scheme is more reliable and robust compared to spatial technique. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) work as a medium for embedding process [6].

A. Different Image Steganography Techniques

(i) LSB (Least Significant Bit)

It is the most common and easiest method for embedding process and hence used widely. Here, secret information gets embedded within the Least Significant Bits (LSBs) of cover-image. Changes made to LSBs of image do not make much induce much difference due to which image looks almost same to original image. In 24 bits image, 3 LSB bits of pixel are used for embedding and these represent red, blue and green components of pixel.

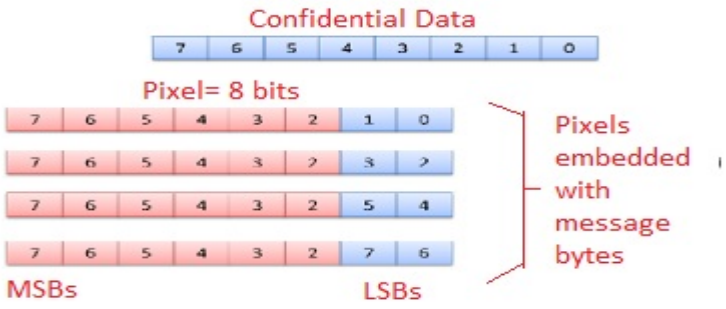

Figure.7. LSB technique

(ii) Parity Checker Method

In this type, concept of even and odd parity is focused. '0' is embedded within pixel when parity is odd, i.e. number of -1- bits are odd while '1' is inserted if parity is even, and i.e. number of -1- bits is even. At receiver's end, if parity is odd then message bit is taken '0' else if parity is even then message bit is taken as '1'.

(iii) Masking and Filtering

If cover image is 24-bit or grey scale image then this technique is used. Just like watermarking, this method also adds watermark of secret data over the image but in a hidden form. Masking is a process of changing luminance of masked area in cover image [7]. This technique is more robust when performing transformation like cropping and compressing are essential to be performed.

(iv) Gray Level Modification (GLM) [6]

While using GLM, gray levels of cover image are modified for embedding and secret data is mapped to pixels of cover image. This technique uses concept of odd and even number while mapping. It is one-to-one mapping process. A mathematical function is used here to select pixels in image for embedding and after comparing gray levels of those pixels with secret data the mapping is done.

(v) Discrete Cosine Transform (DCT)

DCT is a technique where the image is divided into different frequency bands, such as high, medium and low frequency bands before embedding process. After this the data is watermarked to selected band frequency. Mostly middle or medium band is selected for watermarking as it does not allow watermark to scatter within visible parts of image. Also low frequency bands are more secure to noise and compression issues compared to middle and high bands.

III. BENEFITS AND DRAWBACKS OF IMAGE STEGANOGRAPHY

Benefits: The hidden text using steganography does not stand out to human eyes. It can be done using innocuous contents for cover like protocols and images. Watermarking can be implemented with the help of Image stenography. Valuable information like pins of credit cards, person's bank account details, debit card numbers etc. can easily be hidden among digital images.

Drawbacks: Small details like GPS location or e-mail address is easy to send through digital images due to their small size but if a large document like a book is to be send then that's a tough job to do. If intruder gets to know about secret transmission going on then he/she can easily decode simple steganographic data, hence, cryptography is to be combined for safe transmission.

IV. APPLICATIONS OF IMAGE STEGANOGRAPHY

Image steganography is applicable at many places. It can be used to perform confidential communication or storing of secret data. It is combined with watermarking to provide copyright protections. Steganography is broadly used in spheres suchlike military and defense, banking sector, marketing business, E-commerce, media and database systems. Steganography is also spreading in biometrics' field for creation of secure as well as robust systems. It is also used in industries as a mechanism to prevent privacy breechings.

V. CONCLUSION AND FUTURE WORK

This paper is reviewed work of basics of image steganography with different types of techniques pre-owned for it. Amongst all of them, LSB is efficient and widely used for steganography. We also discussed different factors that affect steganographic system like, PSNR, MSE, SNR, robustness etc. The paper provides a big support to initiators going to start work in this field. In further, more advanced techniques like hybrid cryptography with steganography, LSB in detail and enhancing security of data will be studied.

VI. REFERENCES

[1] Ghania Al Sadi, "Image Steganography Approach", International Journal of Computer Science and Mobile Computing (IJCSMC), ISSN: 2320-088X, Volume 4, Issue 8, pg. 166-169 (August 2015).
[2] Nitin Jain et al., "Image Steganography using LSB and Edge-Detection Technique", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume 2, Issue 3 (July 2012).
[3] C. P. Sumathi et al., "A study of Steganographic Techniques used for Information Hiding", International Journal of Computer Science and Engineering Survey (IJCSES), Vol. 4, No. 6 (Dec 2013).
[4] Champakamala et al., "Least Significant Bit Algorithm for Image Steganography", International Journal of Advanced Computer Technology (IJACT), ISSN: 2319-7900, Volume 3, number 4.
[5] Stuti Goel et al., "A Review of Comparison Techniques of Image Steganography", Global Journal of Computer Science and Technology, ISSN- 0975-4350, Volume 13, Issue 4(year 2013).
[6] Anjali Tiwari et al., "A Review on Different Image Steganography Techniques", International Journal of Engineering and Innovative Technology (IJEIT), ISSN- 2277-3754, Volume 3, Issue 7 (January 2014).
[7] Banasthali Vidyapith, "Image Steganography Techniques: A Review Article", ACTA Technica Corviniensis- Bulletin of Engineering, ISSN: 2067-3809, Fascicule 3 (July–September 2013).
[8] Rakhi and Suresh Gawande, "A Review on Steganography Methods", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), ISSN: 2320-3765, Volume 2, Issue 10 (October 2013).
[9] Jasleen Kour and Deepankar Verma, "Steganography Techniques: A Review Paper", International Journal of Emerging Research in management and Technology, ISSN: 2278-9359, Volume 2, Issue 5 (May 2014).
[10] AshadeepKaur et al., "Review Paper on Imge Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, Volume 6, Issue 6 (June 2016).
[11] R. Poornima and R. J. Ishwarya, "An Overview on Image Steganography", International Journal of Computer Science and Engineering Survey (IJCSES), Volume 4, No. 1 (February 2013).
[12] "https://en.wikipedia.org/wiki/Steganography", [Online].
[13] "https://en.wikipedia.org/wiki/Cryptography", [Online].
[14] Mohammed Salem Atoum and Mohammed M. Abu Shquier, "A Various Issues in Image Steganography that Using LSB Technique", International Journal of Computer Networks and Communications Security, Volume 3, No. 9, pg.: 363-366 (September 2016).
[15] "https://en.wikipedia.org/wiki/Steganalysis",[Online]