Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 4, April-2017

Survey: Image Steganography and its techniques

Viral R. Goti[1], Prof. Nisha Shah[2]

Department of Information Technology (System and Network Security),
Sardar Vallabhbhai Institute of Technology, Vasad, Gujarat, India-388306

Abstract *- "Steganography" is a Greek origin word which means "hidden writing". Steganography is the most important area of research in recent years. Steganography is an art and the science of embedding secret information into cover media like, text, image, video, audio or multimedia content for the military communication, authentication, security and many other purposes. It deals with the ways of hiding the secret communication message and its existence from the third person. In image steganography, secret communication is achieved through embedding a secret message into an cover media and generates a stego-media having hidden secret information. There are several image steganography techniques are used each have its advantage and disadvantage. This paper discusses various image steganography techniques such as least significant bit, discrete wavelet transformation, Pixel value differencing, discrete cosine transformation, Masking and filtering etc.*

Keywords: *Steganography, stego-image, Least significant bit, Pixel value differencing Spatial domain methods, Transform domain techniques, Distortion techniques.*

1. Introduction

With the development of computer and the rise of internet, the information is easily transferred from one location to another. But in some cases it is needed to keep the information must travel secretly. Steganography is art and science in we can hide secret information in other kind of cover media[1]. Existing methods in image steganography focus on increasing storage capacity of secret information. Steganography is gain its importance due to the growth and secret communication of potential computer users over the internet. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the secret communicated message[3]. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, in military communication, authentication and many other purposes. In image Steganography, secret communication is achieved to embed a message into cover image and generate a stego- image. One of the grounds discussed in information security is the exchange of information through the cover media. Many different techniques like cryptography, encryption etc. have been developed to encrypt and decrypt information in order to keep the contents of message secret. But steganography have an advantage over these techniques, it keeps the existence of the message secret as well as secret the information. Steganography is the process of hiding the one information into other sources of information like text, image, audio or video file, so that it is not visible to the natural view[2] Steganography is the art and science of invisible communication of messages by hiding information into other information. In image steganography the information is embedded into innocent looking cover image and the message implanted image is called a stego-image. In history there are several secret communication methods are used like undetectable inks , microdots , character organization , digital signatures, spread spectrum etc. that conceal the existence of information. But now day's digital methods are used so the steganography is mostly used on digital information[5]. There are various steganography techniques used based on the information to be hidden. In this paper we describe brief review of many image steganography techniques.

2. IMAGE BASED STEGANOGRAPHY TECHNIQUE

Image steganography, the embedding of data into digital cover pictures, represents a threat to the protecting of secret information and the gathering of intelligence. An image steganographic methods are one kind of steganography systems, where the secret information is hidden in a digital cover image. On other site of user can then use a proper embedding procedure to recover the hidden secret message from the cover image. The original image is called a cover image in steganography, and the message-embedded image is called a stego-image. Following figure shows the diagram of image based steganography[11].

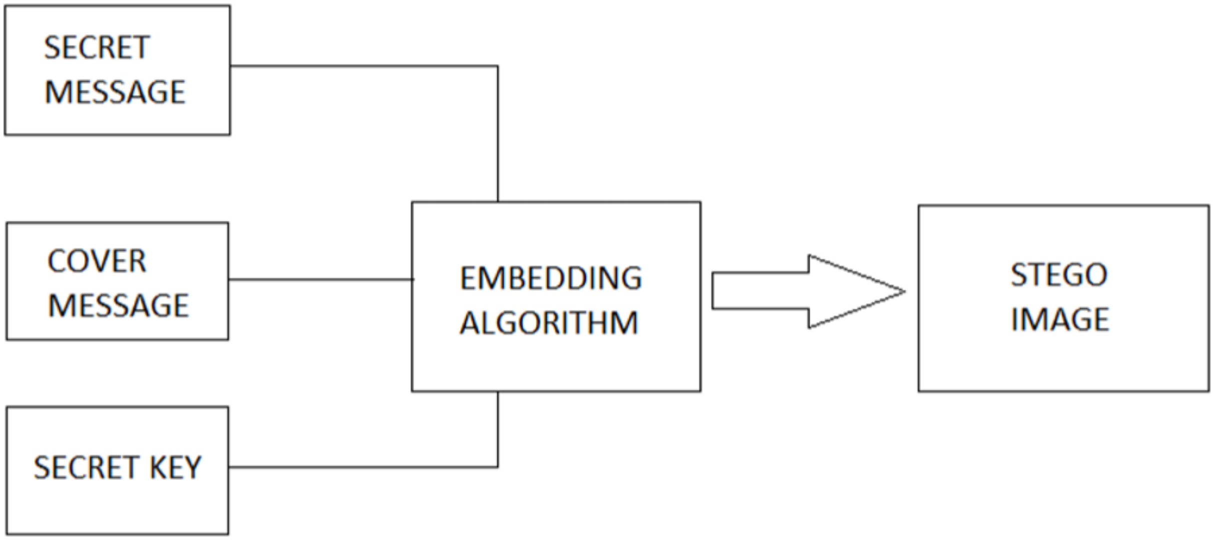

Fig 1: Image steganography diagram

There is many type of image steganography techniques which is describe here:

2.1. Spatial domain Steganography:

In spatial domain steganography method, for the data hiding some bits are directly changed in the image pixel values. Most used method in this category is least significant bit (LSB).Spatial domain techniques are classified into following:

2.1.1 Least Significant Bit (LSB):

LSB insertion is a simple method for embedding information in a cover image. Digital images used as cover image are mainly of two types- 24-bit images and gray-scale images. In 24-bit images we can embed three bits of secret information in each pixel of image. In gray-scale images we can embed one bit of secret information in each pixel. After applying the LSB algorithm the image obtained having secret message is called stego image. LSB method replaces the least significant bit of the pixel with the secret information to be hidden in to the cover image. Since LSB is replaced there is no effect on cover image and hence third person will not get the idea that some message is hidden behind the cover image. However a little change in level of intensity of original and modified pixel, but it cannot be detected visually to the human eye. The following example explain how the letter A can be hidden into the three pixels i.e. eight bytes of a 24-bit image[3].

Pixels: (00100111 11101011 11001010)

(00100111 11011000 10101001)

(11001000 00110111 11011001)

A: 010100111

Result: (00100110 11101011 11001010)

(00100111 11011000 10101000)

(11001001 00110111 11011001)

The very important advantage of LSB method is very easy to implement and high message payload and there is very less chance of degradation of quality of original image. The disadvantages are that the information can be easily extracted or destroyed by attacks and it is less robust, vulnerable to image manipulation.

Advantages of LSB technique are:

1. Degradation of the original cover image is not easy.
2. Imperceptibility is high.
3. Payload capacity is high.

Disadvantages of LSB technique are:

1. Robustness is low.
2. Hidden data can be destroyed by simple attacks.

2.1.2 Pixel Value Differencing (PVD):

In PVD method, 8-bit images is used as a cover media as the secret data. It was originally proposed to hide secret information into 256 gray scale images. The technique is based on the fact that human eyes can easily observe small bit changes in the smooth areas of image but they cannot observe very larger changes at the edge areas in the images. PVD uses the difference between the image pixel and its neighbor to determine the number of embedded secret bits. The larger the difference, the more secret bits can be embedded into the cover image.

This techniques is proposed to enhance the embedding capacity without improper visual changes in stego image. But the disadvantage of the method is sometimes the pixel value in the stego image may change to range 0-255 which leads to improper visualization of the stego image**.**

2.1.3 Histogram Shifting Method:

Histograms are used to represent graphical visualization of image. It represents the pixel value and density at a particular pixel. It plots the pixel for each part of the image. A histogram is useful to identify pixel distribution, density of colors and tonal distribution. A histogram provide as highest and lowest pixel values of image in the graph. In histogram the highest value is called maxima and the lowest value is called minima. When the pixel value is modified for embedding process it should not cross the minima and maxima limit. There are several algorithm which supports histogram functionality in order to manipulate the image. The number of the pixels constituting the peak in the histogram of a cover image is equal to the hiding capacity because a single peak in a cover media is used.

2.2 Transformation Domain Technique:

Transformation domain methods hides secret message in the special areas of the cover image which makes them more robust against various image processing methods like compression and cropping. The basic method used for hiding secret information is to transform the cover image, tweak the coefficients and then insert the transformation.

Advantages:

- Imperceptibility is high.

- Robustness capacity is high.

Disadvantages:

- Payload capacity is low.

Transformation domain techniques are following:

2.2.1 Discrete Fourier Transformation Technique:

In DFT all the insertion of hidden secret message is done in the frequency domain. The Discrete Fourier Transform (DFT) of spatial value f(x, y) for an image of size M×N is defined in equation[3].

$$f(u,v)=\frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\ e^{-12\nabla \quad \frac{ux}{M}+\frac{vy}{N}}$$

…………. (1)

DFT converts the cover image from spatial domain to frequency domain. And each pixel in spatial domain is transformed into two parts: (1) real and (2) imaginary part. The hidden secret message bits are inserted in real part of frequency domain excluding first pixel. During the decoding of the message image from spatial domain is transformed to frequency domain. After applying DFT and extraction algorithm the original image is retrieved.

2.2.2 Discrete Cosine Transformation (DCT) Technique:

It is transforms the image from spatial domain to frequency domain and separates the image into sub-bands with respect to visual quality of the image, like. Low, middle and high frequency components as shown in fig. 2. In figure FL and FH is used to denote the lowest frequency components and higher frequency components. FM is used as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image [3].

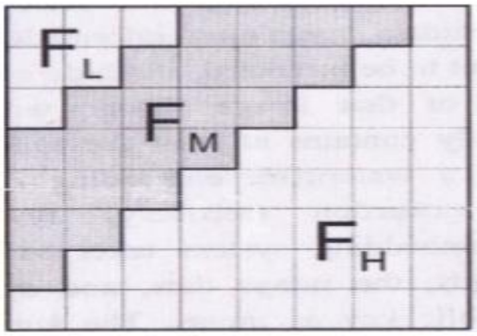

Fig 2: DCT regions

2.2.3 Discrete Wavelet Transformation Technique:

The Discrete Wavelet Transformation (DWT) Technique is idea in the applications of the wavelets. The standard technique of storing in the least significant bit of pixel still applies but the only difference is the information is stored into the wavelet coefficients, instead of changing the bits of actual pixels in the image. The DWT splits the signal into two parts: high and low frequency. The information about the edge component is in high frequency part. And the low frequency part is further split again into high and low frequency parts[3].

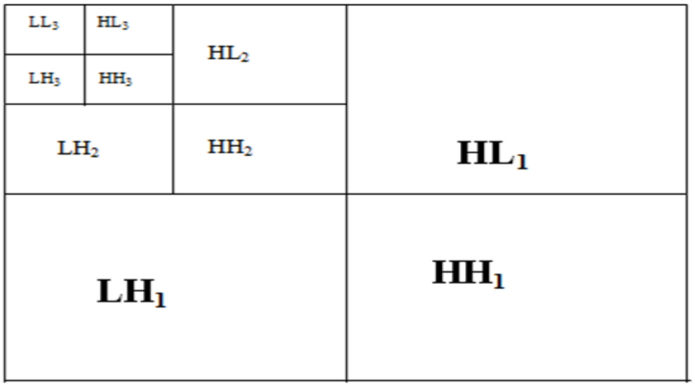

Fig 3: Three phase decomposition using DWT

2.3 Distortion Technique:

Using signal distortion information is stored in distortion techniques. In these method require the knowledge of the original cover image in the decoding process. The encoder applies series of modifications to the cover image. The decoder functions is use to check for the various differences between the original cover image and decoded cover image to recover the secret message.

2.4 Masking and Filtering:

This method is usually applied on 24 bits or 8-bit images. It hides secret information by marking an image, similar to paper watermark. This method actually extends an image data by masking the secret data over the original data as rather than to hiding secret information inside of the data. These method embed the secret information in the more significant areas of the image than just hiding it into noise level. This method is more robust than LSB modification with respect to compression. The main disadvantage of this technique is that it can only be used on 8-bit images and restricted to 24-bit images.

Advantages of Masking and filtering:

1. This method is much more robust than LSB replacement with respect to compression.

Disadvantages:

2. Techniques can be applied only to 8-bit images and restricted to 24 bits.

Conclusion

Image steganography is the art of hiding secret information through the digital cover images. In this paper we have discussed about image steganography and its techniques. Every technique have its own importance. Every technique use for hiding the secret data in cover image.

Acknowledgment

Second author of the paper offers the sincere gratitude to the Head of the Department and faculty members in Department of Information Technology of Sardar Vallabhbhai Patel Institute of Technology for the constant encouragement and unparalleled support provided throughout the period of this research work.

Reference

[1] V. Lokeswara Reddy, Dr. A. Subramanyam, A.P. Dr.P. Chenna Reddy,’’ Implementation of LSB Steganography and its Evaluation for Various File Formats”, Int. J. Advanced Networking and Applications 2011

[2] V.Nagaraja, Dr. V. Vijayalakshmib and Dr. G. Zayarazc,’’ Color Image Steganography based on Pixel Value Modification Method Using Modulus Function”, ScienceDirect 2013

[3] Amritpal Singh, Satinder Jeet Singh,” An Overview of Image Steganography Techniques”, IJECS 2014

[4] Aditya Kumar Sahu, Gandharba Swain,” A Review on LSB Substitution and PVD Based Image Steganography Techniques”, IJEECS 2016

[5] Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni,” Comparison of different techniques for Steganography in images”, International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2014

[6] Gandharba Swain, Saroj Kumar Lenka,” Classification of Image Steganography Techniques in Spatial Domain: A Study”, IJCSET 2014

[7] Saurabh V. Joshi, Ajinkya A. Bokil, Nikhil A. Jain, Deepali Koshti,” Image Steganography Combination of Spatial and Frequency Domain”, International Journal of Computer Applications 2012

[8] Gunjan, Er. Madan Lal,” Investigation of Various Image Steganography Techniques in Spatial Domain”, IJCERT 2016

[9] Rejani. R, Dr. D. Murugan, Deepu.V.Krishnan,” Comparative Study of Spatial Domain Image Steganography Techniques”, Int. J. Advanced Networking and Applications 2015

[10] Vikshit Rabara, Aditya Goswami,” A Survey of Image Based Steganography”, IJCES

[11] Harjit Singh,” Analysis of Different Types of Steganography”, IJSRSET 2016

[12] L.Baby Victoria, Dr.S.Sathappan,” A Study on Spatial Domain and Transform Domain Steganography Techniques used in Image Hiding”, international journal of innovative technology and creative engineering 2015

[13] Nishant Pattani, Kishan Patel, Nirmal Patel, Kashyap Pandya, Amruta Patel,” Survey on Image Steganography Techniques”, IJRES 2015