Chapter 20
Digital Image Steganography: Survey, Analysis, and Application

Chitra A. Dhawale
P. R. Pote College of Engineering and Management, India

Naveen D. Jambhekar
S. S. S. K. R. Innani Mahavidyalaya, India

ABSTRACT

Digital data transmitted over the insecure communication can be prone to attacks. Intruders try various attacks to unauthorized access of the confidential information. The Steganography is such as security system that provide the protection to the images, text and other type of data digitally transferred through the data communication network. This chapter elaborates the basics of Digital Image Steganographic techniques from ancient era to digital edge, types of images used for the steganography, payload used for the steganography, various attacks and different algorithms that can provide the information security. The performance analysis of the various Digital Image Steganographic algorithms are discussed. The current applications and their necessities are discussed in this chapter.

INTRODUCTION

Digital data in the form of text, images, audio and video are transmitted over the internet by means of communication links. The confidentiality of secret data should be preserved from intruders. Steganography contains a group of methods with which different algorithms are available to embed the secret data under the cover medium such as image, without any detectable indications on the cover image. Many algorithms are designed to provide the security for the communication of data over the Internet. The good steganographic algorithm is identified by the performance of the algorithm measured with the help of the parameters such as PSNR, MSE, robustness and capacity to hide the information in the cover image. This chapter explores the steganographic methods used from many years, the methods used currently and the capabilities of steganography in future. The crucial part of the steganographic algorithms are the carrier and its payload. There are various types of carriers available for the steganographic applications.

DOI: 10.4018/978-1-7998-1763-5.ch020

Steganography is the technique that covers the confidential data under the cover medium such as image, without reflecting any clue on the cover image (Chan & Cheng, 2004). Secrete Message transmission is possible by the technique steganography with the help of entities such as a secret message, message carrier and the embedding algorithm who embed the secret message in the cover message i.e. image. The Message is the secret data which is being hidden and carrier is the entity that covers the secret message (Valandar, Ayubi & Barani, 2015). Using the image steganographic method, the secret message is covered by an image in such way that the secret message can be easily extracted as well as the cover image does not lose its visibility (Bender, Morimoto & Lu, 2010). The variations are done slightly, that do not reflect the visual changes in the image.

The mathematical techniques, available in the cryptography have some limitations and can prone to crack mathematically. The image steganography is more secure, but the processing and extraction of the secret message from the cover image need some more processing time. The good steganographic algorithms are able to hide the sensitive data under the cover medium such as image, without remaining any noticeable clue to the intruders (Sun & Liu, 2010). The strength of the steganographic algorithms is to keep the confidential information under an image such a way that, no any steganalysis method, or tool extracts the original message from the cover image without the proper stego key (Mishra, Tiwari & Yadav, 2014).

In the spatial domain, the spatial based methods carried out by the image pixel base using the techniques such as Least Significant Bit (LSB) insertion, SVD and spread spectrum methods. In the frequency based methods, the Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT), Discrete Fourier Transformation (DFT) and Integer Wavelet Transformation (IWT) steganographic transformation based methods hide secret image i.e. the payload to another cover image (Verma, 2011).

The efficiency of the above steganographic algorithms can be analyzed by comparing the cover image with the stego image. This comparison is carried out by calculating the parameters viz. Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE) with the help of programming the code in MATLAB (Gonzalez, Woods & Eddins, 2010). Figure 1 shows the digital image steganographic algorithms.

The steganographic algorithms are classified using text, digital image, audio, video, internet protocols and 3d domain as shown in the Figure 1. This chapter explores the Digital Image Steganographic Algorithms by evaluating using image (spatial) domain and transform (frequency) domain. The spatial or image domain consists of the LSB insertion, PVD and spread spectrum methods while the transform or frequency domain consists of DWT, DCT, DFT and IWT methods which are discussed below (Barni, 2001).

Effective and efficient steganographic algorithms are those who hide the sensitive data under the cover medium such as image, without leaving any detectable clue to the intruders. The strength of the steganographic algorithms is to keep the confidential information under an image such a way that, no any steganalysis method, or tool extracts the original secret message from the cover image without finding right stegokey (Denemark, Boroumand, &Fridrich, 2016). Stegokey is used to merge the secret data under the cover image. The stegokey is unique and used for encryption and same for decryption. This stegokey must be preserved by both sender and receiver (Khan et al., 2014). Recently, many researchers have worked on steganography and written the benefits of the different steganographic algorithms.

Steganography is a group of methods used for securing the secret information under the cover medium such as an image using some translation rules. Here the translation rules merge the selected text into the image, that makes the simple text secure and no one can easily plunder the secret information.