ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

Steganography: Cause and Effect

Harmanpreet Kaur

Department of Computer Science, Guru Nanak Dev Khalsa Girls College, Bathinda, Punjab, India

Abstract: With the development of computer and internet in different areas of life and work, the security has a vital role in networking. Information security is transfer the information through the different network media, so the different methods like steganography, cryptography, coding etc.are used. Steganography is the method to hide the message and has two types of material message is the secret data which should be hidden and carrier has material which has the message. This paper studies the various types & methods of steganography such as image, audio/video and text/document and to conceal the methods.

Keywords*:* Steganography, Spatial domain technique, Transformation domain, LSB, ISB**.**

I. INTRODUCTION

Steganography is the art of invisible information or images in other information. The word Steganography is retrieved from the Greek word stegano means hide and grafia means writing this means covered writing. This method creates a secret path for sending data like file, image, music, sound, text, video-clips etc. invisibly. This technique prevents unauthorized users to access the data. The main goal of Steganography is to hide information well enough such that the unintended recipients do not suspect the steganographic medium of containing hidden data Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible [1].Cryptography was developed as a technique for secure the message in secret form which have produced to various different methods to encrypt and decrypt data. Steganography and Cryptography are similar methods both are used to invisible information. But there is a major difference is that the Steganography does not disclose any unauthorized user regarding the hidden information. The attackers cannot try to decrypt the data. For hide the information in images, there are a number of Steganography techniques which are more complex and the requirement of the application different methods are used.

II. CATEGORIES OF STEGANOGRAPHY

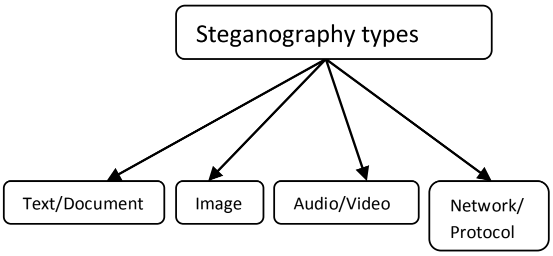

Figure 1: Steganography types

a. Text/Document

Hiding information covered in the document or text file. In this method, the secret data is hidden inside the every word of the message. Various number of methods are using for hide data in the document/text file like Formed Based Method, Random and Statistical Method and Linguistic Method.

b. Image

It consists of hide the data in the form of two types like Transform Domain and Image domain. Transform domain applies image transformation and manipulation of algorithm and Image domain applies bit insertion and noise manipulation of a covered image.

c. Audio/video

This type involves cover data in audio/digital video files. Various sound files WAV, AV, MP3 and video files MP4, MPEG etc. In general, the discrete cosine transformation alters the values to hide the data in the form of images which are in video and these are invisible by the human eyes.

d. Network or Protocol

In OSI layer Model, hide the information using various protocols like TCP, UDP, ICMP, IP etc. OSI Layer protocols are used for hide the data from unauthorized users using the covert channels.

III. STEGANOGRAPHY TECHNIQUES

a. Spatial Domain Technique

This method of steganography is also called the grey level mapping whose deals with pixels of image directly. Spatial domain techniques like logarithmic transforms, power law transforms, histogram equalization are based on the direct manipulation of pixels in the image. These techniques use the pixels gray levels and their color values directly for encoding the message bits [2]. This method concern with alter the grey level values of individuals pixels and it comes overall contrast of the whole part of the image. Generally, two techniques log transformation and power law transformations are used. Spatial domain technique manipulate the conceal image pixel bit values to embed the secure information. Secure bits are written those are directly to the cover image pixel bytes.

1)Least Significant Bit

In the spatial domain technique, the least significant bit is one of technique has lowest significant bit in the byte value of the image pixel and embeds the secret

DOI 10.17148/IJARCCE.2015.47117

information in the least significant bit of the pixel values of the cover image. It exploits the fact that the levels of precision in many image formats [3].

2) Intermediate Significant Bit

ISB technique requires four bytes of pixels of secret data and LSB eight bytes of pixels to store 1 byte of secret data. During the encryption process, the size of the secret data or image is less than the cover image when secret image are convert them into grey scale images.ISB used to change the watermarked image pixels by new pixels and secure the watermark data against attacks and new pixels are closed to original pixel to improve the picture quality.

This method is based on the testing the value of the watermark pixel according to the range of each bit-plane. This technique is based on the robustness and maintains the quality of watermarked image.

b. Transformation domain technique

Transformation domain techniques also called the frequency domain technique which is based on the manipulation of the orthogonal transform of the image not a image itself. Orthogonal transform has two components magnitude and phase. The magnitude deals with frequency content and phase consists of restore the image which is back to the spatial domain. Alpha rooting technique is one of the most useful techniques of transformation domain technique.

c. Spread Spectrum Technique

Using the spread spectrum technique, the secret data is spread over a wide range band of frequencies. It can be attained by modulating the narrowband waveform with a wideband waveform. Narrow band signal frequency is low after spreading and then it is very difficult to detect. In spread spectrum communications, the signal is energy inserted into any one frequency is too undersized to create a visible artifact and the secret image is scattered over a wide range of frequencies that it becomes robust against many common signal distortions.

d. Distortion Technique

During the decoding process, this technique has need to knowledge of the cover image where the decoder function is used to check the difference between the original cover image and distorted cover image which has to store the secret message. The encoder adds sequences of changes to cover image then the information is used regarding the signal distortion. Using this technique, a stego object is created by applying a sequence of modifications to cover image [4]. Modification sequence is matching the secret message which is used to transmit.

e. Masking and filtering

Similar to paper watermarks, this method is used to hide information by making an image and restricted to 24-bit and grey scale images. Copyright, ownership or license etc information's are digital watermarks. This can be achieved for example by modifying the luminance of parts of the image [5]. In this technique the hidden message is more integral to the cover image then the hiding data in the noise level. Masking method adds the duplicate to the hidden information then masking technique is more suitable with lossy JPEG images and protect against different kinds of processing as cropping, rotating and compression etc.

IV. APPLICATION OF STEGANOGRAPHY

Steganography can be used in various applications such as in military, defence and intelligence organizations, smart id proof cards which have personal details etc. In medical, patient details are also embedding with in image. Steganography provides confidential communication, secret data storing. Several applications like E-Commerce media, database systems, and digital water marking are generally used.

V. CONCLUSION

In this paper, we discuss about steganography, its types and technique. First we had a see at the types of steganography and then it different methods like spatial domain, transformation domain techniques. The data is broken down in blocks which have relatively decreasing lengths and each block concealed in the cover media using control highly secure key. At last, the steganography is used to convert communication for transfer confidential information over a communication channel.

REFERENCES

[1] Shashikala Channalli, Ajay Jadhav, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1 (3), 2009, 137-141

[2] Ms.G.S.Sravanthi,Mrs. B.Sunitha Devi, S.M.Riyazoddin & M.Janga Reddy, "A Sapatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", Global Journal of computer science and technology graphics & Vision, Vol.12,issue 15 version1.0,year 2012

[3] Champakamla.B.S, Padmini.K, Radhika.D.K Asst Professors, "Least Significant Bit algorithm for image steganography", International Journal of Advanced Computer Technology. Vol.3.

[4] Mehdi Hussain and Mureed Hussain," A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[5] Masoud Nosrati, Ronak Karimi and Mehdi Hariri, "An introduction to steganography methods", World Applied Programming, Vol. (1), August 2011.

[6] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON-2008, November 2008, pp. 1-6.

DOI 10.17148/IJARCCE.2015.47117