Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on Image Steganography

Rashi Singh
Student
Deptt. Of Comp. Sc. & Engg.
G.I.T.M, Gurgaon, India

Gaurav Chawla
Associate Professor
Deptt.Of Comp. Sc.& Engg.
G.I.T.M, Gurgaon, India

Abstract: This paper gives a review of steganography, its various techniques, its advantages and disadvantages, applications, it's merging with cryptography techniques .Today's the rise of the internet become the most important factor of information technology and communication but along with this the threat of information security increases. It's become very important to give security to your data so that no unauthorized person can access it. The steganography is a powerful security tool with which we can hide a secret message inside an object. The object can be text, image, audio or video.

Keywords: Steganography, Spatial Domain Methods, Transform Domain Technique, Masking, Stego-Image.

I. INTRODUCTION

Steganography is a unique technique of hiding data in some medium so that it doesn't arouse suspicion to the hackers. The term steganography has been derived from two Greek words Steganos and graphia, where "steganos" means covered or secret and "graphic" means writing or drawing. So steganography is covered writing. The main purpose of steganography is to hide the fact of communication. In this the sender embedded its message into the text, image, video, or audio file so that hackers will not be aware of the message. It is not a new technique it is very old. The most popular stegnographic methods used by spies include invisible ink and microdots. People used etching messages in wooden tablets and covered with wax. They used tattooing a shaved messenger's head, letting his hair grow back and then saving it again when he arrived at his contact point to reveal the message.

II. WORKING OF STEGANOGRAPHY

Some terms which are used in steganography are:

- **Cover Image**: The medium in which information is to be hidden. It may be an audio, video, image or a text file.
- **Stego-image**: A medium within which information is hidden.
- **Message**: The data to be hidden or to be extracted.
- **Key**: It's a secret value which help in encoding or extraction of data, without which data cannot be encode and extract.

For steganography we must have some message to be embedded and a cover image in which message is to be hide. The chosen cover image can be of any size -8 bit format or of 18 bit, 24 bit, 32 bit, 36 bit and can be in any format either jpeg, gif, bmp, png etc. More the size it is easier to hide the message and much bigger message can be hide but large image sending on the web will make it suspicion . we must have a key which is used to select the random pixels on which data is to hide. Now by using three of these a stego image is generated which is send to another person. Now on the receiver side the stego image is processed and extraction of message takes place by the help of secret key. The key is the one by which receiver knows the position of the pixel on which message is embedded.

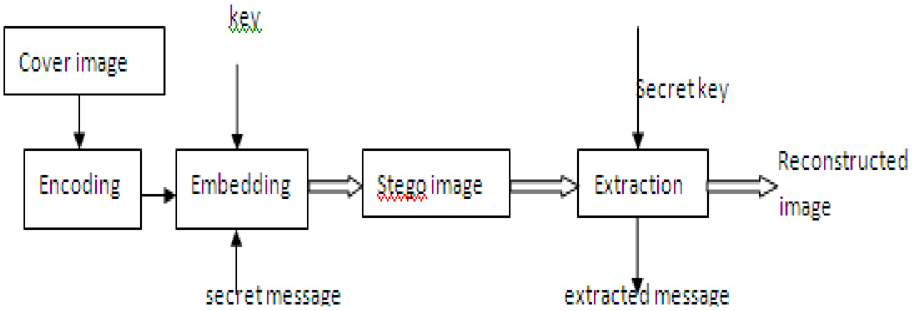


Figure 1: General Block Diagram of Steganography

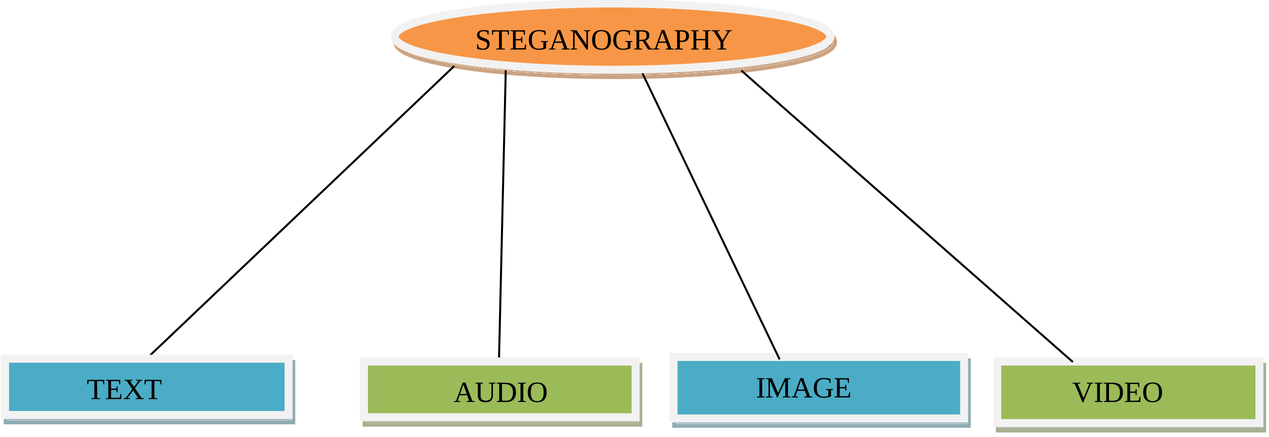
III. RELATED WORK

Neil F. Johnson, Sushil jajodia et. Al[1] , hey discuss different techniques of steganography and file compression, masking & filtering techniques. Mamta janesa, parvinder sing sandhu et al[3] ,They discuss the design of a robust image steganography technique based on LSB insertion & RSA encryption technique. Piyush marwaha, paresh marwaha[4], They propose the concept of multiple cryptography where the data will be encrypted into a cipher & the cipher will be hidden into a multimedia image file in encrypted formal, visual steganography algorithm will be used to hide the encrypted data. Feng Pan, Jun Li et al[7] ,They present an image steganography method which utilize horizontal pixel & vertical pixel difference, in the horizontal direction they use high quality model function method for two pair of pixel embed message they use PVD method. Pfitzmann & westfield[8],They proposed a particle algorithm for embedding JPEG image that would provide high steganographic capacity without sacrificing security. Ming.chen,z.Ru.et al[9] , They have explain many stenography tools which are capable of hiding data with an image. These tools can be classified into five category on their algorithm i.e are spatial domain based tools, transform domain based tools, document based tools, file structure based tools, video compress encoding and spread spectrum techniques. Hassan mathkour, Btool Ai.sadoon et.[10] , They discussed several steganography techniques with an emphasis on image steganography they list a set of criteria to look into the strength & weaknesses of presented techniques.they also discussed & compared various steganography tools. Implemented a tool exemplifying its process. Ge Huayong,Huang Mingsheng et. Al[11], They illustrate concept and principle of steganography and steganalysis, spatial domain and transform domain embedding method are generalized. Then the performance specification of image steganography is discussed. Sueed sarreshtedari & shahrokh Ghaemmaghami[12], They proposed steganography algorithm works on the wavelet transform coefficients of the original image to embed the secret data.

IV. STEGANOGRAPHY

Steganography is classified as -

- ***Text-based Steganography*** - In which the message to be sent is embedded in a text file by formatting it based on line-shift coding, word-shift coding, feature coding etc. Reformatting of the text destroys the embedded content hence the technique is not robust.
- ***Audio Steganography*** - Alters audio files so that they contain hidden messages. The techniques are LSB manipulation, phase coding and echo hiding.
- ***Image Steganography*** - Hides message in the images. This technique is the most popular because of the fact that almost no perceivable changes occur. In images after hiding a large amount of data with wide variety of available images. Depending on the data hidden in the pixels directly or in the coefficients obtained after a suitable transform domain like FFT, DFT or DWT leads to spatial domain Steganography and frequency domain Steganography. Some of the commonly used methods of embedding payload in cover image are least Significant Bits (LSB) substitution in which the LSBs of cover image pixel are altered to hide the payload and more data can be hidden in edges.
- ***Video Steganography*** - Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video format.



V. STEGANOGRAPHY TECHNIQUES

- ***Spatial Domain Methods:*** There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are unpredictable to human eyes,
- ***Transform Domain Technique:*** This is a more complex way of hiding information in an image. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the

transform domain. The advantage of this technique over spatial domain techniques is that they hide information in areas of the image that are less exposed to compression, cropping, and image processing. All transform domain techniques are not dependent on the image format and they may run on lossless and lossy format conversion.

- ***Distortion Technique**:* In this technique the decoding process is based on the decoding function. The decoding function checks difference between original cover image and the distorted cover image to restore the secret message. In this a stego- image is created by applying sequence of modification to cover image. The message is encoded at some random chosen pixels. If the stego image is different from cover image at the given message pixel, the message bit is "1".otherwisw message bit is "0".
- ***Masking and Filtering:*** These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. Advantages of Masking and filtering Techniques: This method is much more robust than LSB replacement with respect to compression as information is hidden in visible part of the image.

VI. APPLICATION OF STEGANOGRAPHY

- ***Copyright Protection**:* A secret copyright notice can be embedded inside an image to identify it as intellectual property. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified.
- ***Feature Tagging**:* Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.
- ***Secret Communications**:* In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use of stenography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive I formation can be transmitted without alerting potential attackers or eavesdroppers.
- ***Digital Watermark:*** A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal.
- ***Use by terrorists:*** Steganography on a large scale used by terrorists, who hide their secret messages in innocent, cover sources to spread terrorism across the country. It come in concern that terrorists using steganography when the two articles titled “Terrorist instructions hidden online” and “Terror groups hide behind Web encryption” were published in newspaper.

VII. STEGANOGRAPHY SOFTWARES

Existing LSB Base Software

One of the popular and oldest techniques used to hide message in digital image is to hide it in the least significant bit (LSB) of pixel value. Some of the software are given below-

a. Mandelsteg by Henry Hastur
b. Steg by the JPEG group
c. S-tool by Andrew Brown
d. Gzip by Andrew Brown
e. Hide seek by Colin Maroney
f. Wbstego by Werner bailer
g. Enhanced LSB method

a) Mandelsteg by Hastur

Mandelsteg stand for “Mandelbrot Steganography” it uses the GIF format files to store the secret information. It store the secret information in 640*480 mandel.gif file.

b) Steg by the JPEG Group

Steg compresses image files using the JFIF format of the JPEG standard.

It has produced two executables

- Cjpeg: To compress image files using the JPEG standard.
- Djpeg: To decompose a JPEG file.

c) S-Tools by Andrew Brown

S-Tools for windows is the most versatile Steganography tool of all that we have tested. It uses GIF and BMP format files to store the secret information; S-Tools applies the LSB method to both image and audio files.

d) Gzip by Andrew Brown

Gzip is a loss less file compression utility. Two executables are provided Gzip and Unzip for compression and decompression. To hide the information Gzip include the –s option in the command line, to hide a file in the compress file. For unhiding and decompression unzip also include –s option in the command line.

e) Hide and seek by Colin Maroney

Hide and seek by Colin Maroney uses GIF file format it store the hidden information. It consist two executable Hide and Seek. Hide is used two hide secret information from the file secret.txt in giffile.gif. Seek is used to retrieve the information from giffile.gif and produces a file called secret.txt.

f) Wbstego

Wbstego is LSB inserting software; it is a tool that hides any type of file in bitmap images, text files, HTML files or Adobe PDF files. The file in which you hide the data is not optically changed. It can be used to exchange sensitive data security or to add hidden copyright information to files.

g) Enhanced LSB Method

This technique make use of 5th, 6th, 7th ,8th bit of random chosen pixel value of image to insert the message bit in such manner that effective change in pixel value in range +1 to-1. Hence image quality is same as in case of least significant bit insertition. The message can be inserting at any bit position in the image pixel either at

- 5th ,6th, 7th bit
- 7th, 8th bit
- 8th bit

VIII. CONCLUSION

The Paper gives the review of Steganography, its history and basic working of Image Steganography along with various insertion techniques used in Image Steganography, such as Spatial Domain Methods, Transform Domain Technique, Distortion Technique Masking and Filtering. The paper also covers steganography software and different applications such as secret communication, copyright protection, digital watermarking.

REFERENCES

[1] Adel Almohammad "*steganography-based secret and reliable communications: improving steganographic capacity and imperceptibility*" a thesis submitted for the degree of doctor of philosophy, department of information systems and computing, brunel university, august,2010.

[2] Arvind Kumar and KM. Pooja "*steganography- a data hiding technique*", international journal of computer applications (0975 – 8887) volume 9– no.7, November 2010.

[3] M. Bachrach, and FY. Shih, "*image steganography and steganalysis*," wiley interdisciplinary reviews: computational statistics, vol. 3, pp. 251-9, 2011.

[4] Cheddad, A.J. Condell, K. Curran, & P. Mc Kevitt. "*a skin tone detection algorithm for an adaptive approach to steganography*". Signal processing, 89(12): 2465-2478. Doi: 10.1016/j.sigpro.2009.04.022, 2009.

[5] *T. Morkel , J.H.P. Eloff and M.S. Olivier "An Overview of Image Steganography"*

[6] Amanpreet Kaur, Renu Dhir, and Geeta Sikka *"A New Image Steganography Based On First Component Alteration Technique"* (IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 3, 2009

[7] Mehdi Kharrazi, Husrev T. Sencar and Nasir Memon *"Image Steganography : Concepts and Practices "Polytechnic University, Brooklyn, NY 11201, USA*

[8] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn *"Information Hiding A Survey"*Proceedings of the IEEE, special issue on protection of multimedia content, 87(7):1062{1078, July 1999.

[9] Ankita Agarwal *" Security Enhancement Scheme for Image Steganography using S-DES Technique"* International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 4, April 2012

[10] Adel Almohammad *"Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility"* A thesis submitted for the degree of Doctor of Philosophy, Department of Information Systems and Computing , Brunel University, August, 2010.

[11] Rajkumar Yadav *"Study of Information Hiding Techniques and their Counterattacks: A Review Article" ,* International Journal of Computer Science & Communication Networks, Vol 1(2), 142-164, Oct-Nov 2011