IJTRET
"Voice of Innovative Minds"

International Journal of Trendy Research in Engineering and Technology
Volume 4 Issue 6 Oct' 2020
ISSN NO 2582-0958

A SURVEY ON IMAGE STEGANOGRAPHY TYPES AND HIDING TECHNIQUES

[1]B. Chitradevi, Research Scholar, Research & Development, Periyar University, Salem.
[2]Dr.S. Manikandan, Professor & Head, Department of Computer Science and Engineering,
Sriram Engineering College, Perumalpattu, TamilNadu

citradevi.b@gmail.com

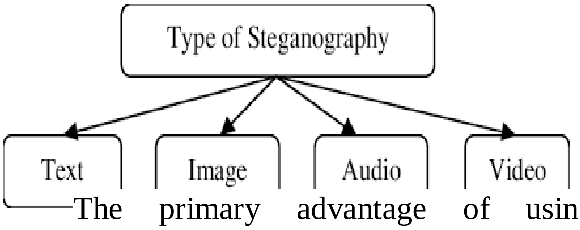
Abstract

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word *steganography*is derived from the Greek words *steganos*(hidden or covered) and the Greek root *graph*(write).Steganography is dedicated for covert communication. It changes the image in such a way that only the sender and the intended receiver can detect the message sent through it. Since it is invisible, the detection of secret data is not simple.

Keyword: Steganography, Image, Audio, Text, Encrypt, Hiding.

I. Introduction

Digital watermarking, steganography and Reversible Data Hiding (RDH) are the types of data hiding approaches. Watermarking is a sequence of digital bits placed in a digital cover file that recognizes the file's copyright information.



The primary advantage of using steganography to hide data over encryption is that it helps obscure the fact that there is sensitive data hidden in the file or other content carrying the hidden text. Whereas an encrypted file, message or network packet payload is clearly marked and identifiable as such, using steganographic techniques helps to obscure the presence of the secure channel.

In steganography, the cover file does not hold any significance after extraction of secret data. Whereas in RDH the cover file also holds the information like secret data. The RDH allows one to embed a relatively large amount of data into an image in such a way that the original image can be reconstructed from the marked image. This makes it an ideal technique for applications where one wants to store metadata into the cover signal, while recover the original signal without loss after data extraction.

Steganography Works

Steganography replaces unneeded or unused bits in regular computer files (Graphics, sound, text) with bits of different and invisible information. Hidden information can be any other regular computer file or encrypted data.

Steganography differs from cryptography in a way that it masks the existence of the message where cryptography works to mask the content of the message.

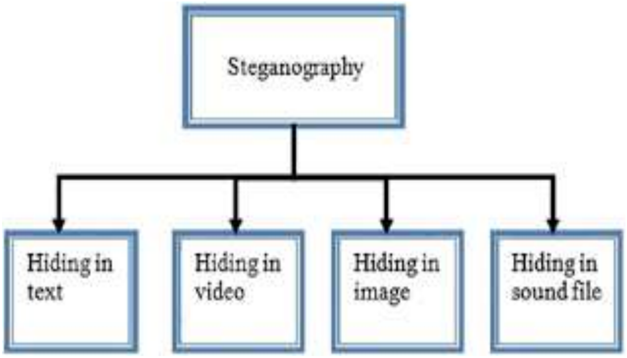
Steganography sometimes used in conjunction with encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden information is not seen.

II. Types of Steganography

There are different ways to hide the message in another, well known are Least Significant bytes and Injection.

When a file or an image is created there are few bytes in the file or image which are not necessary or least important. These type of bytes can be replaced with a message without damaging or replacing the original message, by which the secrete message is hidden in the file or image.

Another way is a message can be directly injected into a file or image. But in this way the size of the file would be increasing accordingly depending on the secrete message



(i). Text Steganography: It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message. Numbers of methods are available for hiding data in text file. Themethods are Format Based Method, Random and Statistical Method,and Linguistics Method.

(ii). Video Steganography: It is a technique of hiding any kind of files or data into digital video format. In this case video is used as carrier for hiding the data. Generally discrete cosine transform alter the values which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye.

(iii). Image Steganography:Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

(iv). Audio Steganography: It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. The methods areLow Bit Encoding, Phase Coding and Spread Spectrum.

(v). Network or Protocol Steganography: It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there exist covert channels where steganography can be used

Steganography in Image

Digital images are the most widely used cover objects for steganography. Due to the availability of various file formats for various applications the algorithm used for these formats differs accordingly.

An image is collection of bytes containing different light intensities in different areas of the image. When dealing with digital images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. Both have advantages and disadvantages 8-bit images are a great format to use because of their relatively small size. The drawback is that only 256 possible colors can be used which can be a potential problem during encoding. Usually a gray scale color palette is used when dealing with 8-bit images because its gradual change in color would be harder to detect after the image has been encoded with the secret message. 24-bit images offer much more flexibility when used for Steganography.

Large amount of data can be encoded in to 24-bit images as it is compared to 8-bit images. The drawback of 24-bit digital images is their size which is very high and this makes them suspicious our internet due to their heavy size when compared to 8-bit images.

III. Image Steganography Algorithms:

i. Least significant bit insertion
ii. Masking and filtering
iii. Redundant Pattern Encoding
iv. Encrypt and Scatter
v. Algorithms and transformations

i. Least significant bit insertion

Least Significant Bit (LSB) insertion is most widely known algorithm for image steganography, it involves the modification of LSB layer of image. In this technique, the message is stored in the LSB of the pixels which could be considered as random noise. Thus, altering them does not have any obvious effect to the image.

ii. Masking and filtering

Masking and filtering techniques work better with 24 bit and grey scale images. They hide info in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking the images changes the images. To ensure that changes cannot be detected make the changes in multiple small proportions. Compared to LSB masking is more robust and masked images passes cropping, compression and some image processing. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, lossy JPEG images.

iii. Redundant Pattern Encoding

Redundant pattern encoding is to some extent similar to spread spectrum technique. In this technique, the message is scattered throughout the image based on algorithm. This technique makes the image ineffective for cropping and rotation. Multiple smaller images with redundancy increase the chance of recovering even when the stegano-image is manipulated.

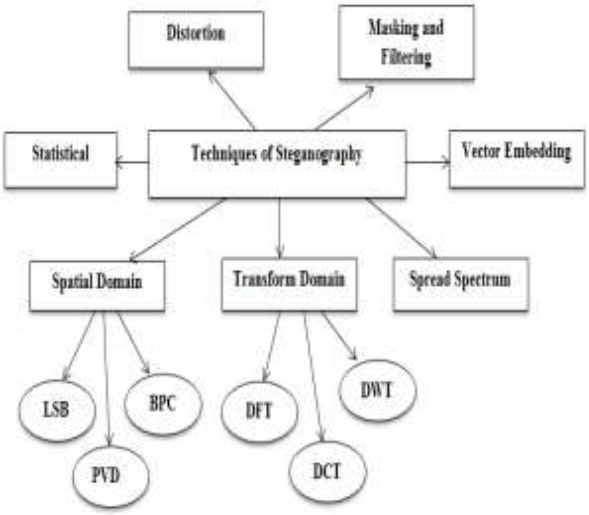
iv. Encrypt and Scatter

Encrypt and Scatter techniques hides the message as white noise and White Noise Storm is an example which uses employs spread spectrum and frequency hopping. Previous window size and data channel are used to generate a random number. Andwithin this random number ,on all the eight channels message is scattered throughout the message. Each channel rotates swaps and interlaces with every other channel. Single channel represents one bit and as a result there are many unaffected bits in each channel. In this technique it is very complex to draw out the actual message from stegano-image. This technique is more secure compared to LSB as it needs both algorithm and key to decode the bit message from stegano-image. Some users prefer this method for its security as it needs both algorithm and key despite the stegano image. This method like LSB lets image degradation in terms of image processing, and compression.

v. Algorithms and transformations

LSB modification technique for images does hold good if any kind of compression is done on the resultant stego-image e.g. JPEG, GIF. JPEG images use the discrete cosine transform to achieve compression. DCT is a lossy compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to calculate DCT.

Techniques of Steganography



Application of Steganography

- Confidential Communication and Secret Data Storing
- Protection of Data Alteration
- Access Control System for Digital Content Distribution
- E-Commerce
- Media
- Database Systems.
- digital watermarking.

Features of Image Steganography:

1) Transparency: The steganography should not affect the quality of the original image after steganography.

2) Robustness: Steganography could be removed intentionally or unintentionally by simple image processing operations like contrast or enhancement brightest gamma correction, steganography should be robust against variety of such attacks.

3) Data payload or capacity: This property describes how much data should be embedded as a steganography to successfully detect during extraction.

IV. Various methods of image steganography:

i) Data Hiding Method: hiding the data, a username and password are required prior to use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image. This method is used to hiding the existence of a message by hiding information into various carriers. This prevents the detection of hidden information.

ii) Data Embedding Method: For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image. This is to ensure the integrity and confidentiality of the data. The process of embedding the message inside the image, a secret key is needed for retrieving the message back from the image, the secret message that is extracted from the system is transfer into text file and then the text file is compressed into the zip file and zip text file is converting it into the binary codes

iii) Data Extracting Method: It is used to retrieve an original message from the image; a secret key is needed for the verification. And for extracting method, a secret key is needed to check the key is correct with the decodes from the series of binary code. If key is matched, the process continues by forming the binary code to a zipped text file, the unzip the text file and transfer the secret message from the text file to retrieve the original secret message.

Factors Include in Steganography:

(i). Robustness: Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations.

(ii). Imperceptibility: The imperceptibility means invisibility of a steganography algorithm.

(iii). Bit Error Rate: The hidden information can be successfully recovered from the communication channel.

(iv). Mean Square Error: It is computed by performing byte by byte comparisons of the two images.

(v). Peak Signal to Noise Ratio: The image steganography system must embed the content of hidden information in the image so that the quality of the image should not change.

Example of Image Steganography

Original image

Original image + hidden data

V.Conclusions

In this paper, basics of Steganography concepts are described. In this basically Image steganography techniques are discussed. All the techniques discussed in this paper are able to secure the hidden data. On the other hand some algorithms have a very high time complexity and very less amount of data stored in the images. So, there is a need to develop efficient and accurate Steganography algorithms, either by combining the existing techniques or by developing new techniques. It helps in detecting terrorist activities on web.

References:

1. *Gandharba Swain et al. ,Classification of Image Steganography Techniques in Spatial Domain: A Study, International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345, Vol. 5, No. 03 Mar 2014, Pp- 219*
2. *Harpreet Kaur and Jyoti Rani, A Survey on different techniques of steganography, MATEC Web of Conferences, DOI: 10.1051/ 57, 02003 (2016), ICAET 2016*
3. *Mr. Jayesh Surana, Aniruddh Sonsale, Bhavesh Joshi, Deepesh Sharma and Nilesh Choudhary, Steganography Techniques, 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939, Pp-989*
4. *Masoud Nosrati et al., An introduction to steganography methods, World Applied Programming, Vol (1), No (3), August 2011, ISSN: 2222-2510, Pp 191-195*
5. *Navneet Kaur and Sunny Behal, A Survey on various types of Steganography and Analysis of Hiding Techniques, International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014, ISSN: 2231-5381 ,Pp 388-392*
6. *kaur Amandeep kaur, manpreet, "Improved SecurityMechanism of Text in Video using SteganographicTechnique," Int. J. Adv. Res. Comput. Sci. Softw.Eng., vol. 7782, no. 5, (2014)pp. 44–51*