Review Paper on Different Types of Steganography

Rupali Khot, Prof.A.S.Patil

Padmabhooshan Vasantdada Patil Institute of Technology, Pune, MS-India

Abstract - To provide security in modern communication media steganography is used. Steganography is a technique of hiding message from third party. It is the technique of covering one medium of communication within another medium. Different mediums available are text, image, audio and video. Digital images are mostly used because of their frequency on the internet. Redundant bits of data from hidden message are replaced by embedding process which will create stego image. This paper reviews the different types of give steganography.

Keyword: *steganography, Audio message, image, least significant bit (LSB) method.*

I. INTRODUCTION

Steganography is an important area of research in recent years. It plays a key role in hiding data. Data is hidden inside cover and that cover is called as carrier file for example text, audio, video, and image.

II. STEGANOGRAPHY

A. Steganography System

In steganography system steps can be involved as follows. There is one cover and message file in which message file can be covered inside of cover file, by using steganography tool one single stego file obtained which can be used for hiding messages.

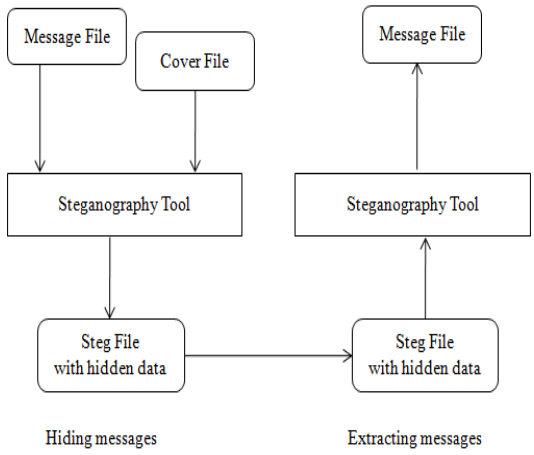

Fig.1: Steps involved in steganography system

While extracting message the same stego file can be used as output to extract message by using steganography tool, finally message file obtained as shown in above Fig.1

B. Steganography Classification:

Depending upon this carrier file, steganography is classified as:

i. Text Steganography

In text steganography formatting or by changing certain characteristics of textual elements can be changed. It consist of line-shift coding, word-shift coding and feature coding.

ii. Image Steganography

In this steganography, Image is commonly used cover file. There are different file formats are available for digital images and for these file formats different algorithms are exist such as least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations.

iii. Audio Steganography

In audio steganography, secret message is embedded into digitized audio signal which result slender shifting of binary sequence of the equivalent audio file. There are a number of methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

iv. Video Steganography

Video files consist of assortment of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. Advantages of using video steganography is that large amount of data that can be hidden inside the cover file and it is the fact that it is flow of images and sounds.

C. Principles of Steganography

Again steganography is classified as pure steganography, secrete key steganography and public key steganography.

In pure steganography there is no former replacement of information among the two communicating parties which will depends on secret throughout insignificance. This means that the algorithms not widely known.

Secret key steganography uses a widely known algorithm. It uses a secret key which is decided by the two parties communicating. This key is needed to both embed and extract

the hidden information, and if the proper key is not used, it cannot be known if data is actually hidden in a given cover object.

Pure steganography entail the sender using recipient's public key to embed the information, which can be only be detected using the recipient's private key.

D. Image Encoding Techniques and Methods

To hide the information in images following types are used.

- Least Significant Bit Insertion
- Masking and Filtering

These types can be applied to various images, with varying degrees of accomplishment. These get suffers to varying degrees from operations performed on images such as cropping or resolution decrementing or decreases in the color depth. Similarly, image hiding steganography methods are of two types as follow.

- Spatial domain steganography
- Frequency domain steganography

Spatial Domain Steganography

In Spatial domain techniques, the intensity of the pixels is used to embed messages directly. Least Significant Bit (LSB) is the extensively used spatial domain steganography technique. In LSB bits of a message are hidden in the pixels of image. But in this technique while doing image compression the hidden data may get lost. Loss of data that may have insightful information. LSB has been enhanced by using a Pseudo Random Number Generator (PRNG) and a secret key in order to have confidential right to use to the hidden information. The embedding process starts with deriving a seed for a PRNG from the user password. Then these bits are stego image has less PSNR value than LSB techniques.

Frequency Domain Steganography

In frequency domain, images are first altered and then the message is embedded in the image. When the data is embedded in frequency domain, the hidden data resides in more vigorous areas spread across the entire image and provides better confrontation against statistical attacks. Many techniques are used to transform image from spatial domain to frequency domain. The commonly used technique in image processing is the 2D discrete cosine transform. In this technique first the image is divided into 8×8 blocks and then DCT transformation is applied on each block. According to the frequency value DCT set the pixel of image. The data bits are embedded in the low frequency coefficients of DCT. In this technique stego image PSNR value is generally low.

Least Significant Bit Insertion

It is a common simple approach to embedding information in a graphical image file. Regrettably, it is extremely susceptible to attacks such as image exploitation. Thus the overall image distortion is kept to a minimum while the message is spaced out over the pixels in the images. This technique mechanism is preeminent when the image file is superior to the message file and if the image is grayscale.

A simple alteration from a GIF or BMP format to a lossy firmness format such as JPEG can wipe out the hidden information in the image. LSB techniques is applied to each byte of 24-bit image. Three bits can be encoded into each pixel. Each pixel is represented by three bytes. Any changes in the pixel bits will be indiscernible to the human eye. For example, the letter X can be hidden in three pixels. Assume the original three pixels are represented by the three 24-bit words below (11100111 10001001 11111000) (00100111 11001111 11001001) (11011011 01111101 11001110) the binary value for the letter X is (111001010). Inserting the binary value of A into the three pixels starting from the top left byte.

Pixels:
(11100111 10001001 11111000)
(01100101 11001111 11001001)
(11011011 00111111 11001110
A:
(101101100)
Result:
(00100111 11101001 1100100**1**
(00100110 1100100**0** 11101001)
(11001010 00100111 11001000)

The underlined bits are the only bits that actually changed. The improvement of LSB method is that data can be hidden in the least significant and second significant bits and the human eye would be not capable to perceive it. When applying LSB techniques on 8-bit images, it is important that 8-bit formats are not as sympathetic to data changes as 24-bit formats are. Commonly notorious images should not be selected. It is essential to retain information that a change of even one bit could mean the difference between a shade of red and a shade of blue. Such a change would be instantaneously perceptible on the displayed image and is thus undesirable. Therefore data-hiding experts counsel using grey-scale palettes where the differences between shades are not as pronounced.

Masking and Filtering

In this techniques information is hidden by marking an image. By wrappering or masking a soft but detectable signal with another to make the first non-perceptible we exploit the fact that the human visual system cannot detect slight changes in the image. Technically watermarking is not a steganographic form. Masking techniques are more proper for use in lossy JPEG images than LSB insertion because of their

imperviousness to image operations. Masking and filtering techniques is where information is hidden inside of an image using digital watermarks that include information such as copyright, ownership, or licenses. The purpose is different from traditional steganography since it is adding an attribute to the cover image thus extending the amount of information presented.

III. CONCLUSION AND FUTURE WORK

This paper reviewed the main steganographic techniques. These techniques tries to assure the factors of steganographic design such as imperceptibility or undetectability, capacity, and robustness. As LSB techniques have a high payload capacity, they are not succeed to prevent statistical attacks and are thus easily detected. This future work we are going to hide audio in an image file using Least Significant Bit -1(LSB-1), Least Significant Bit-2(LSB-2) based Steganography, LSB with secret key, an improved inverted LSB image Steganography, secret key steganography and run time steganography. The LSB algorithm is implemented in embedding domain in which the secret audio data is embedded into the least significant bits of cover image to originate the stegoimage

IV. REFERENCES

[1] "An effective implementation of LSB Steganography using DWT techniques", K.P.Uday kanth and D.Vidyasagar, June2014.
[2] "An Improved Inverted LSB Image Steganography" Nadeem Akhtar, Shahbaaz Khan, Pragati Johri, IEEE, 2014
[3] International Journal of "Advanced Research in Computer Science and Software Engineering", Steganography Using Various Quantization Techniques",Tara Bansal,Ruuchika Lamba,Volume 3,Issue 7,July 2013.
[4] Steganography in mobile phone over bluetooth Shatha A. Baker1 and Dr. Ahmed S. Nori 2, August 2013.
[5] Research Journal ON "A Proposed Algorithm ForSteganography In Digital Image Based on Least Significant Bit "BY A. E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi, Ahmed.BD, April, 2011.
[6] "Image Steganography : Hiding short audio message within digital image",M. I. Khalil, Reactor physical department, nuclear research center, Atomic energy authority, cairo,Egypt,October,2011.
[7] "A New Approach for LSB Based Image Steganography using Secret Key" S. M. Masud Karim, Md. Saifur Rahman,Md. Ismail Hossain,,IEEE ,December 2011.
[8] Steganography for e-Business: An Offensive Use of Information SecurityToshiyuki ueyoshi and Gopalakrishna Reddy Tadiparthi, 2004.
[9] Steganography in Corporate environment, Joann Kennedy, Toshiyuki Sueyoshiand Gopalakrishna Reddy Tadiparthi, April 9, 2004.