Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

A Survey of Steganography with its Techniques

[1]Zindhu.S, [2]PArockia Valanrani. B
[1,2]Assistant Professor, Department of Computer Science, St. Joseph's College of Arts and Science for Women, (Hosur, Tamilnadu, India)

Abstract - In this period of digital driven world, it is important to secure digital information while communicating across the internet. Steganography is one of the techniques used for this purpose. Steganography is defined as the study of invisible communication. Steganography deals with the ways of hiding the existence of the communication data, in order to make it confidential. It maintains secrecy between two communicating parties. There are different types of Steganography techniques each have their strengths and weaknesses .This paper unfolds the different security and data hiding techniques that are used to implement a steganography such as LSB,ISB,MLSB etc..

Keywords *: Steganography; Embedding; Extraction; LSB*

I. INTRODUCTION

Steganography is the art and science of communicating is such a way that it hides the existence of the communication. Due to development in techniques of the data security, development are made in the field of hacking as well. So, the need of improving data security methods is increasing step by step. Steganography is one of the techniques for securing confidential information across the internet. It hides the existence of the data so that no one can identify its presence. In Steganography the process of hiding information inside any multimedia content like image, video, audio is referred as a "embedding".

II. STEGANOGRAPHY

Steganography is greek word which means secret writing. The word "Steganos" means "covered" and "graphical" means "writing". Accordingly, Steganography is the art of hiding the transmission of secret data. Steganography hides the secret data in a file in such a way that only the recipient knows the existence of message (Provos & Honeyman, 2003). In ancient time, the data was protected by hiding it on the back of wax, writing tables, stomach of rabbits, or on the scalp of the slaves. But now most of the people convey the data in the form of images, video and audio over the medium. Today is the era of digital steganography. Multimedia such as image, audio and video can be used to hide the secret message in form of text from hackers while transmitting it over the internet.

Cover media is the media used to hide the secret message. On the sender side, secret message and cover media act as an input in embedding process. Embedding process refers to the sequence of steps used to hide the message and its output is the steganographic object. Steganographic object must be identical from the cover object because imperceptibility is the first and foremost requirement of the steganography.

Figure 1 shows the basic model of steganography. On the receiver side steganographic objects acts as an input to the extraction process, where extraction process is exactly the reverse of embedding process used to resolve out secret message from the input as an output. (Kaur, Singh, & Girdhar, 2014)

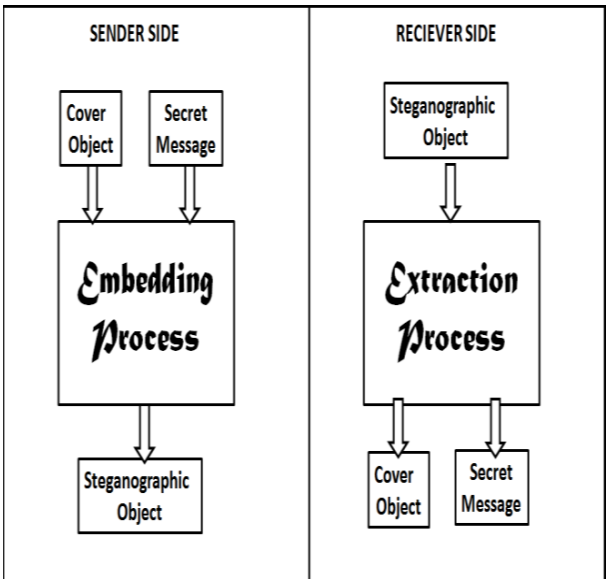

Figure 1: Basic model of digital steganography.

III. TYPES OF STEGANOGRAPHY

A. Text Steganography

It consists of hiding information inside the files. In this , the secret data is hidden at the back of even nth letter of every words of text message. Number of methods are available for hiding data in text file. these methods are 1) Format based method; 2) Random and statistical method; 3) Linguistics method

B. Image Steganography

Hiding the data in the cover object as image is referred to as steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are broadly used cover sources because there are number of bits presents in digital representation of an image. (Gutub, Al-Qahtani, & Tabakh, 2009)

C. Audio Steganography

It involves hiding data in audio files. This method hides the data in WAN, AU and MP3 sound files. There are different method of audio steganography. These methods are 1) low bit encoding, 2) phase coding , 3) spread spectrum.

D. Video Steganography

It is a techniques of hiding files or data into digital video format. In this, video is used as carrier for hiding the data. Usually discrete cosine transmission(DCT) alters the value, that is used to hide the data in each of the images in the video, which is invisible to the human eye. H.264, MP4, MPEG, AVI are the formats used by video steganography.

E. Network or Protocol Steganography

It involves hiding the information by tasking the network and protocol such as TCP,UDP,ICMP,IP etc.. as cover object.

IV. STEGANOGRAPHY TERMINOLOGY

Steganography consists of two terms that is message and cover image. "Message" is the secret data that needs to hide and "Cover Image" is the carrier that hides the message in it.

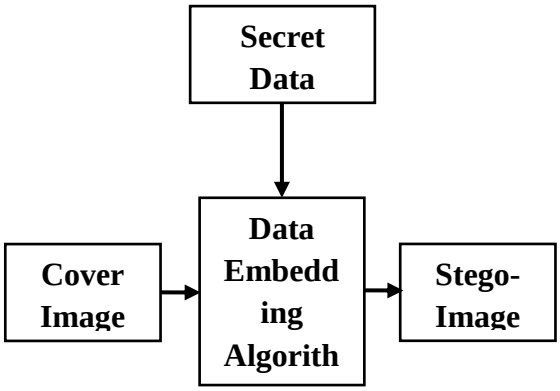

Figure 2: Steganography Diagram

V. STEGANOGRAPHY TECHNQUES

A. *Spatial Domain Methods*

In this, the secret data is embedded directly in the intensity of pixels. Spatial domain techniques are classified into following categories : i) LSB – Least Significant Bit ii) PVD – Pixel Value Differencing iii) EBE – Edges Based data Embedding method iv) RPE – Random Pixel Embedding method v) MPH – Mapping Pixel to Hidden data method vi) Labeling or connectivity method vii) Pixel Intensity method

- **LSB :** This method is commonly used for hiding data. In this the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. After embedding the image obtained is similar to original image because the change in the LSB of image pixel does not bring too much differences in the image. (Yang, et al., 2013) (Kumar & Sharma, 2013)

- **PVD:** In this method, two consecutive pixels are chosen for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serve as basic for identifying whether the two pixels belongs to an edge area or smooth area.

B. *Spread spectrum techniques*

In this method , secret data is spread over a wide frequency band width. The ratio of single noise in every frequency band must be so small that it become difficult to detect the presence of data. Thus it is difficult in military communication .

C. *Statistical Technique*

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no alteration is required .

D. *Transform domain technique*

In this technique, the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain technique are broadly classified as

- Discrete fourier transformation technique (DFT)
- Discrete cosine transformation technique (DCT)
- Discrete wavelet transformation technique (DWT)
- Lossless or then reversible method (DCT)
- Embedding in coefficient bits.

E. *Distortion techniques*

In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to spot the sequence of modification and consequently recover the secret message.

F. *Masking and filtering*

These techniques hide information by marking an image. Steganography only hides the information as watermarks becomes a potion of the images. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This methods basically used for 24-bit and grey scale images.

G. *Digital Watermarking:*

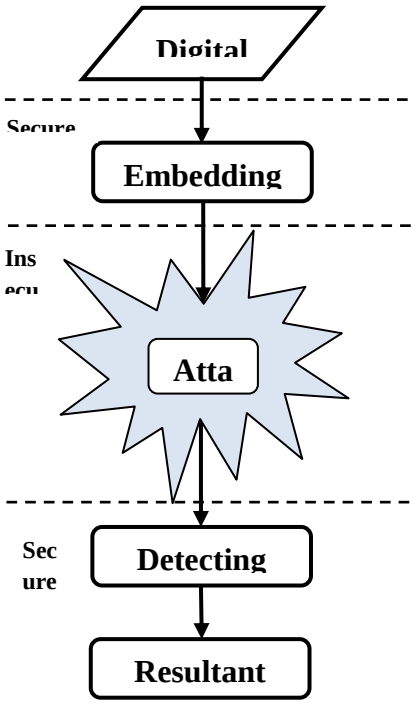

Fig.ure 3: Watermark Lifecycle Phases

Digital Watermarking has been proposed as a technology to ensure copyright protection by embedding an imperceptible, yet detectable signal in digital multimedia content such as images or video. The embedded signal can be used to identify

the rightful owner holding the copyright of the content. The digital watermarking algorithm is composed of three part. A general watermark lifecycle phases is shown in figure 3.

- Watermark embedding algorithm
- Watermark extraction algorithm
- Watermark detected algorithm

A 'digital watermarking' refers to the information to be embedded . The signal where the watermark is to be embedded is called the 'host signal'. In the embedding process, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. This signal is then transmitted or stored.

A watermark attack is an digital data where the presence of a specially crafted piece of data can be detected by an attacker without knowing the encryption key.

Detection (also called as extraction)is an algorithm which is applied to the attacked signal for hacking or destroying the watermark from it. when a watermarking algorithm is robust, then the extraction algorithm should be able to correctly produce the watermarking, though the modifications were strong.

Any watermarking technique has to be evaluated to judge its performance. Three factors must be considered while evaluating a watermarking algorithm.

- **CAPACITY** -The amount of information of that can be put into the watermark and recovered without errors.
- **ROBUSTNESS** - The resistance of the watermark to alteration of the original content such as filtering, compression or cropping.
- **VISIBILITY** - Easily the watermark can be discerned by the user.

These factors are co-dependent and thus increasing the capacity will decrease the robustness or increases the visibility.

VI. FACTORS AFFECTING A STEGANOGRAPHIC METHOD

The effectiveness of any Steganographic method can be determined by comparing stego-image with the cover image. There are some factors that determines the efficiency of a technique. These factors are:

A. Robustness

Robustness refers to the ability of embedded data to remain intact if the stego- image undergoes transformations, such as linear and non-linear filtering, sharpening or blurring, addition of random noise, rotations and scaling, cropping or decimation, lossy compression. (Bailey & and Curran, 2006)

B. Imperceptibility

The imperceptibility means invisibility of a steganographic algorithm. Because it is the first and primary requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye.

C. Payload capacity

It refers to the amount of secret information that can be hidden in the cover source. Watermarking usually embed only a small amount of copyright information, whereas, steganography focus at hidden communication and thus have sufficient embedding capacity.

D. PSNR (Peak Signal to Noise Ratio)

It is defined as the ratio between the maximum possible power of signal and the power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between the original and a compressed image. The higher value of PSNR represents the better quality of the compressed image.

E. MSE (Mean Square Error)

It is defined as the average squared difference between a reference image and a distorted image. The smaller the MSE, the more efficient the image steganography technique. MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count. (Abed, April 2013)

F. SNR (Signal to Noise Ratio)

It is the ratio between the signal power and the noise power. It compares the level of a desired signal to the level of background noise.

CONCULSION

LSB is the most commonly used technique for steganography. Some researcher have also used like Watermarking, distortion techniques are Spatial technique. Security and data hiding techniques are used to implement steganography using LSB, ISB, MSB. They have provided a strong means of secure information transmission. The different security and data hiding techniques are used to implement steganography using LSB, ISB, MLSB.The application of steganography are i) Confidential Communication and Secret Data Storing ii) Protection of Data Alteration iii) Access Control System for Digital Distribution iv) E-Commerce v) Media vi)Database Systems. Vii) digital watermarking.

References

[1] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[2] Abed, D. F. (April 2013). A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography. *IJAIEM, Volume 2, Issue 4,* .

[3] Bailey, K., & and Curran, K. (2006). An Evaluation of Image Based Steganography Methods",. *Journal of Multimedia Tools and Applications, Vol. 30, No. 1,* , 55-88.

[4] Gutub, A., Al-Qahtani, A., & Tabakh, a. (2009). Triple-A: Secure RGB image steganography based on randomization. *Computer Systems and Applications, AICCSA 2009, IEEE/ACS* , 400-403.

[5] Kaur, P., Singh, H., & Girdhar, A. G. (2014). An improved steganographic approach to diminish data

modification for enhancing image quality. *nternational Conference on Medical Imaging,m-Health and Emerging Communication Systems* , 329-333.

[6] Kumar, A., & Sharma, R. (2013). A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique. *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7,* .

[7] N. Provos and P. Honeyman, "Hide and seek: An introduction to

[8] steganography," IEEE Security and Privacy Magazine, vol. 1, 2003.

[9] Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. *IEEE Security and Privacy Magazine* .

[10] Yang, Chunfang, Liu, F., Luo, Xiangyang., Zeng, a., et al. (2013). Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography. *IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1,*

[11] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, *"Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique",* International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[12] 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, (2008) November, pp. 1-6.

[13] C. Christian, "An information theoretic model for steganography,"

[14] Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science, vol. 1525, pp. 306-318, 1998.

[15] P. Kaur, H. Singh, A. Gupta and A. Girdhar, "An improved

[16] steganographic approach to diminish data modification for enhancingimage quality," International Conference on Medical Imaging, m-Health and Emerging Communication Systems, pp. 329-333, 2014.

[17] V. Sharma and S. Kumar, "A new approach to hide text in images using steganography", SIJARCSSE, vol. 3, 2013.