Asian Journal of Convergence in Technology Volume II Issue III
Issn No.:2350-1146, I.F-2.71

Exploring Different Techniques in Steganography and Steganalysis

Saugata Dutta
Research Scholar, OPJS University,
Churu, Rajasthan, India

Dr. Om Prakash
OPJS University,
Churu, Rajasthan, India

Abstract: **Communication has various forms and it is a significant part in our daily life starting from ancient era. Technology changes from time to time so as the mode of communication. Steganography is an art of secret communication. There are various types of steganography like text, images, audio and video. Steganalysis is a study of detecting hidden messages using steganography. This paper intends to explore different techniques used in steganography and steganalysis**.

Keywords—Steganography, Steganalysis, Cryptography, Spatial Domain, Universal Steganalysis.

I. INTRODUCTION

Steganography comes from the combination of Greek word "steganos" meaning cover and "graphein" meaning writing which means cover writing [1]. Steganography is an art of hiding information in other information. Steganography is used to hide the secret message in different mediums such that the information can be passed to intended recipient without suspecting. During ancient times covert communication was done by shaving the head of messenger to mark the messages and then let the hair grow before sending and also there has been evidence for usage of wax tablet. During the world wars, microdots and invisible inks were used. The first recorded use of steganography term was in 1499 by Johannes Trithemius in his book Steganographia. In digital world and modern steganography, the technology and trend has changed. Steganography now being used in text, image, audio and video. In steganography, the original message is hidden in a cover medium through an encoding process and transferred through some communication channel. The output stego file is then decoded at the receiving end. Introduction of encryption is an optional component. Steganalysis is a study where the hidden message in a cover file is being identified. The purpose of steganalysis is to detect and determine the hidden information from the cover medium and extract the information. Steganography differs from cryptography in the sense that in cryptography the data is modified into a form that cannot be known while in steganography the existence of the message is hidden which bypass suspicion. Steganography and cryptography provides different layer of security. However the combination of steganography and cryptography is always a good choice for enhanced security. Steganography is being used in digital watermarking, ecommerce and transport of sensitive data. This paper explores different techniques of steganography and steganalysis.

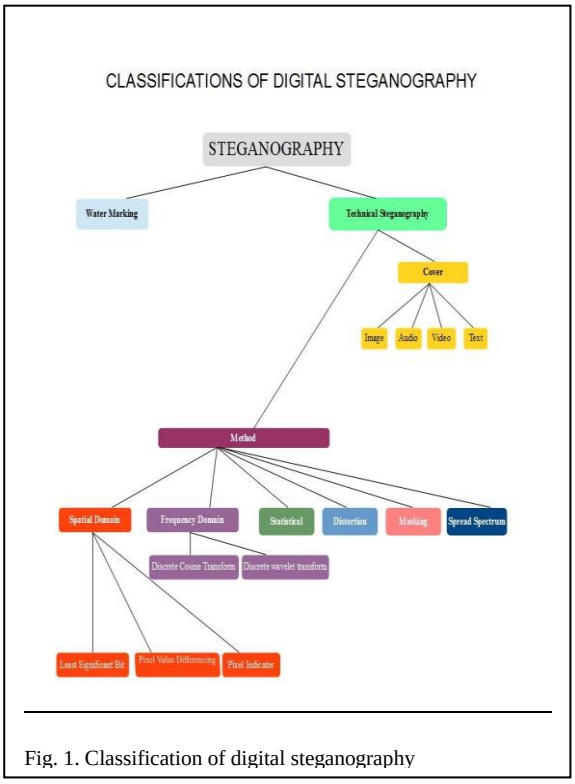

Fig. 1. Classification of digital steganography

II. REVIEW LETREATURE

Mahendra Kumar et al. (2011): proposed a new steganalysis system where a 2-step Markov model was used as feature set for blind steganalysis. Existing techniques have focused one step Markov model and DCT features. The proposed method takes this idea one step further to extract features based on 2-step transition probability matrices [2].

Jiří HOLOŠKA et al. (2011): developed the use of artificial intelligence in steganography detection. The detection is done by feed forward artificial neural network with one hidden layer. This approach shows a promising way of detecting the hidden content in images only [3].

Adel Almohammad et al. (2010): proposed some methods in increasing the capacity of JPEG steganography using 16x16 quantization tables, enhancing the quality of JPEG stego images and increasing the steganographic capacity using optimized quantization tables, investigating the impact of

using chrominance components of steganography, evaluating the reliability of PSNR as a quality measure of stego image and examining the capability of using SOAP message for steganography [4].

Atallah M. Al-Shatnawi et al. (2012): presented, implemented and analyzed hiding of secret message based on searching about the identical bits between the secret message and image pixel values. The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels. The proposed and the LSB hiding methods were implemented to hide the secret message [5].

Michael Morran and George R.S. Weir et al. (2010): explored a series of test to determine the impact of the language processing components in the prototype steganography system. Review of the resultant replacement texts led to the conclusion that default settings would generate acceptably meaningful substitutions in 50%-60% of cases. The remaining cases were likely to be seen as 'odd' by the average reader [6].

Ms B. Veera Jyothi, Dr. S.M. Verma and Dr. C. Uma Shanker et al. (2010): worked on novel data hiding techniques provided by the field of steganography to authenticate an encrypted digital signature, hidden in a digital image. There are no algorithms existing currently to secure email messages which use encryption and image steganography techniques together. They worked on the implementation of an algorithm which uses these two techniques together and analyze the performance of the system [7].

Sabyasachi Pramanik and Samir K. Bandyopadhyay et al. (2014): introduced a new approach to hide data in an image. The advantages in this approach eliminate the use of key and make use of negotiation between sender and receiver. It also eliminates the time complexity of the algorithm, it showed an improve performance in comparison of average and standard deviations between the original image and stego image [8].

Patrick Lloyd et al. (2010): explored the ability to embed covert messages into a voice over IP stream, merely by modifying the SIP and SDP packets which are sent at the beginning of the call. To aid in the ability to monitor the network, a tool has been provided which allows for the capture of packets flowing through the communications network [9].

Natarajan Meghanathan and Lopamudra Nayak analyzed and provided critical review of steganalysis algorithms for three domains which is image, audio and video while that may not be noticed by unintended recipient by applying steganography but can be detected by appropriate steganalysis algorithm [10].

III. TYPES OF STEGANOGRAPHY

On broad category there are four different types of steganography which is being used. Text, Image, Audio and Video. In Text Steganography, information is hidden in the N^{th} letter of word in a text message. Text steganography is now not being used on a larger scale due to its less capacity of hiding data. In Image steganography, the message is hidden in a cover image using an embedded algorithm, the message is then transferred to the recipient as a cover image. The message is received by using an extraction algorithm at the destination end. During this process the unintended recipient will just notice the transmission of the image but won't be able to identify the hidden message inside the image. Audio steganography on the other hand uses masking. The presence of an audible sound gets unnoticed in presence of another louder sound. This property actually allows to select channel in which to hide information. In video steganography, the message is hidden in a cover video file. The main advantage of video steganography is to accommodate more hidden data as compared to audio steganography. There are various tools of steganography to hide messages in a cover medium, some of them are SteganPEG, SilentEye, Outguess, StegHide, Clotho, RT Steganography, QuickStego and OpenStego.

IV. STEGANOGRAPHY TECHNIQUES

The steganographic techniques in this digital age are:

1. Spatial Domain Techniques
2. Spread Spectrum
3. Statistical Technique
4. Transform Domain Technique
5. Distortion Technique
6. Masking and filtering

1. Spatial Domain technique hides the data in the intensity of the pixel. The pixel values are changed when the secret data is embedded into it. This can be further classified into:
   - i. LSB: Least Significant Bit technique is the simplest one used in steganography. This method uses replacement of secret data bits to the least significant bits of image pixels. The resultant is not very different from the original image as the changes in the least significant bit doesn't makes much difference.
   - ii. PVD: In Pixel value differencing two consecutive pixels are selected for hiding the data. In this process the payload is calculated by comparing the difference between the two pixels which serves as a point whether it belongs to smooth area or an edge area. It provides high embedding capacity and imperceptibility to the stego image.
   - iii. PI: Pixel indicator technique provides high data embedding capability and high quality

of stego image and hides data in the difference in pixel values. Although it's more complex way of hiding information in an image.

The advantages of spatial domain techniques are good quality of stego image as against the original image and more information can be hidden in an image. The disadvantages are stego data can be lost with little manipulation on stego image and with simple steganalysis software hidden data can be destroyed with simple attacks.

2. In Spread spectrum technique data is hidden in the frequency which has wide bandwidth. The signal to noise ratio is so small that the presence of data detection is very hard. If some of the data are removed, still there will be a fair chance to recover the data from other bands. It is a reliable approach and used mostly in military communication.

3. In Statistical technique, the message is hidden in changing the various attributes of the cover. The cover is divided into blocks and each block is then embedded with one message bit. The cover block is changed only when the size of the message bit is one.

4. In Transform domain technique the data is hidden in the transform or frequency domain of the cover. The process is complex as compared to spatial domain technique and there are less chances that the data gets destroyed. The data to be hidden is stored in areas where it is less exposed for cropping, compression and processing, Most of the steganographic system now a days operate on this terminology. This can be further classified into Discrete Cosine Transformation (DCT) and Discrete Wavelet Transformation (DWT). In DCT method the uncompressed image is compressed into JPEG type. It is the process in which that data is hidden in the JPEG compression algorithm to transform pixel blocks of the image from spatial domain to DCT coefficients each in frequency domain. Discrete Wavelet transform splits the signal into a set of basic functions. There are actually two types one is continuous and the other is discrete. The information is transferred into the wavelet coefficient of the image [11].

5. In Distortion technique the hidden data is stored by distorting the signal. There are series of modification applied to the cover by the encoder.

6. Masking and Filtering hides information by marking an image. This technique hides information in more important areas than just hiding into noise level.

V. STEGANALYSIS AND TECHNIQUES

Steganography can be misused especially by terrorist and criminals to plot bomb or other type of attacks putting the secret data in image, audio or video and transfer the cover file with secret data and posting them in the newsgroup or video sites. In order to minimize the impact, developed the technique of steganalysis. Steganalysis is the process of detecting and extracting secret messages from steganography.

1. Signature Steganalysis: After the process of steganography, the cover files has some unusual patterns left or property that act as a signature which depicts the possibility of secret information hidden in the cover file.
2. Specific Statistical steganalysis: There are some statistical changes which remains after the steganography process. Statistical steganalysis analyses and detects those statistical changes. Statistical steganalysis is said to be more powerful than signature based steganalysis. There are two types spatial domain and transform domain. In Spatial domain pair of pixels is considered where the difference between them is calculated, it may be a neighboring pixels which may be selected within a block or across the block. Finally after the plotting of histogram the presence of message is shown. In Transform Domain technique frequency counts of coefficients are calculated and histogram analysis is performed.
3. Universal Steganalysis: Specific steganalysis techniques results well on specific method applied and fails with other methods. In order to overcome the situation universal steganalysis is used. Universal steganalysis is a two class pattern classification to classify the test image either a cover or a stego image. There are two parts of classification one is feature extraction and the other is pattern classification. In feature extraction some unique statistical properties are created. These attributes are known as features. The extracted features must be sensitive to the embedding artifacts. Image quality metrics, wavelet decompositions, moment of image statistic histograms, Markov empirical transition matrix, moment of image statistic from spatial and frequency domain, co-occurrence matrix are some of the feature extraction methods. In Pattern classification the images are classifieds into class depending on their feature values.

There are various steganalysis tools that available to detect the presence of hidden information in cover file. StegDetect, StegSecret, JPSeek, StegBreak, StegExpose are some of them.

VI. CONCLUSION

This paper explored various techniques of steganography and steganalysis. There are numerous method discussed which has their individual advantages and limitations and also depicts how one has a precedence over the others. There is an old physics theory "For every action, there is an equal and opposite reaction". The various steganographic techniques throws light on the development of steganographic softwares which provides more robustness and reliable in hiding information. At the same time the steganalysis techniques developed for destroying the steganography showed development too. We explored various techniques of steganography and steganalysis which helped in developing advanced softwares using these technologies which can be used in confidential communication and secret data storing, protection of data alteration, access control system for digital content distribution, E-Commerce, Media, Database systems and Digital watermarking in more advanced manner and artificial intelligence. For misuse of the mentioned usages, steganalysis can be used to detect and extract. The development is ongoing process and continued to be so.

ACKNOWLEDGEMENTS

I am thankful to my project guide who has supported me enormously and also my sincere thanks to professors and friends for the encouragement.

REFERENCES

[1] http://en.wikipedia.org/wiki/Steganography

[2] Kumar, Mahendra. (2011). Steganography and Steganalysis of Joint Picture Expert Group Images, Doctor of Philosophy, University of Florida, United States.

[3] HOLOŠKA, Jiří. (2011). Artificial Intelligence applied on crypto analysis aimed on revealing weakness of modern cryptology and computer security, Dissertation Thesis, Tomas Bata University, Zlin, Czech Republic.

[4] Almohammad, Adel. (2010). Steganography-Based secret reliable communications: Improving steganographic capacity and imperceptibility, Doctor of Philosophy, Brunel University, United Kingdom.

[5] Al-Shatnawi, M. Atallah. (2012). A New Method in Image Steganography with improved image quality. Applied Mathematical sciences. 69 (79). 3907-3915

[6] Morran, Michael. And Weir, R.S. George. (2010). An Approach to Textual Steganography, Department of Computer and Information Sciences, University of Strathclyde, Glasgow, United Kingdom.

[7] Jyothi, B. Veera. Verma, S.M. and Uma Shanker, C. (2010). Implementation and Analysis of Email Messages Encryption and Image Steganography schemes for Image Authentication and Verification. International Journal of Computer Applications. 5 (5). 22-27

[8] Pramanik, Sabyasachi. and Bandyopadhyay, K. Samir. (2014). An Innovative Approach in Steganography. Scholar Journal of Engineering and Technology. 2 (2B). 276-280

[9] Lloyd, Patrick. (2010). An Exploration of Covert Channels within Voice Over IP, Master of Science in Network and System Administration, Rochester Institute of Technology, Rochester, United States.

[10] Meghanathan, Natarajan. and Nayak, Lopamudra. (2010). Steganalysis Algorithms for detecting the hidden information in image, audio and video cover media. International Journal of network Security and its application. 2 (1). 43-55

[11] Saddaf rubab and M Younus. Improved Image Steganography Technique for Colored Images using Wavelet Transform. International Journal of Computer Applications 39(14):29-32, February 2012. Published by Foundation of Computer Science, New York, USA.