A Review on Steganography and Steganalysis

Ramandeep kaur, Arshdeep Singh

Abstract— Steganography is a technique to hide/protect the information. Many people are using this technique to hide their malicious data, so that such data can not be intercepted easily. This paper deals with a review on various Stegangraphy and Steganalysis Techniques .Different papers related to steganography, classification of steganography, video steganography were studied and reviewed. The aim is to study and compare basic techniques of steganography and steganalysis to detect the hidden information.

Index Terms— Steganography, Steganalysis, Least Significant Bit, color model, Secret message,Hidden writing, Video Steganography, pvd based steganography.

1 Introduction

THE Information security is of great importance in today's time. Steganography is a method for information security, which have both advantages and disadvantages depending on how the person is using it. Different terrorist organizations use steganography to hide their information as they have to face well equiped Government security forces. So a technique called staganalysis is used to identify the images from the terrorist that contain a secret message.

In this paper different steganography and steganalysis techniques such as video steganalysis, PVD based content adaptive image steganography, Pixel group trace model based quantitative steganalysis etc. furthermore this paper gives short description of several steganalysis tools and attacks against steganography.

2 Related Work

The art of embedding secret data into common digital media, which also conceals the existence of hidden message is called steganography[1]. On the basis of pixel group trace model two quantitative steganalysis method are proposed for two typical MLSB steganography paradigms, The pixel group trace model traces the transition relationship among the possible structure of pixel group's value by some trace pixel group subset[4].

2.1 Classification

A. Based on detection capabilities (Chandram ouli,2003):
1. Passive Steganalysis: It focuses on revealing the presence of hidden message.
2. Active Steganalysis: It aims at estimating some important parameters of the embedding method.

B. Based on objectives of steganalysis(Luo et al., 2008)
1. Targeted Steganalysis: It is designed for detecting specific steganographic algorithm.
2. Blind Steganalysis: It is designed to detect message independent of the embedding algorithm.

Chunfang Yang, Fenlin Liu, Xiangyang Luo, and Ying Zeng(2012) "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography" This paper represents a pixel group trace model to analyze MLSB (Multiple least significant bits) steganography. On the basis of pixel group trace model two quantitative steganalysis methods are proposed for two typical MLSB steganography paradigms. The pixel group trace model traces the transition relationship among the possible structures of pixel group's value by some trace pixel group subsets. From the transition probability matrix among trace subsets and the symmetry of regular and singular poxel group sets , the estimation equations of embedding ratio are derived. The experimental results show that the proposed steganalysis method can estimate the low embedding ratio with smaller error.

Xikai Xu, Jing Dong, Wei Wang and Tieniu Tan(2013) "video steganalysis based on the constraints of motion vectors"The prime focus of this paper is to detect data hiding in motion vectors of compressed video and to propose a new steganalytic algorithm based on the mutual constraints of motion vectors. By using three functions, the constraonts of motion vectors are analyzed and formulyzed and then statistical features are extracted on the basis of these functions. Also a calibration method is incorporated for improved detection accuracy.

Xiaolong Li, BinLi, XiangyangLuo, BinYang, Ruihui Zhu (2013) "Steganalysis of a PVD-based content adaptive image steganography" PVD (pixel value differencing) is a technique for content adaptive syeganohraphy, in which secret data are embedded into the differences pf adjacent pixels. The method proposed by Luo et al exploits a pairwise modification mechanism to reduce the distortion. This work explains that by counting the differences of adjacent pixels in both vertical and horizontal directions, a folded difference histogrqm is generated and Luo et al's PVD based method may arise significant artifact to this histogram which can be exploited for reliable detection.

- *Ramandeep kaur is Assistant professor at AIET, Faridkot. E-mail:rkaur2310@gmail.com*
- *Arshdeep singh is currently pursuing masters of technology in computer science engineering in PTU jalandhar, India. E-mail: arsh.sra01@gmail.com*

Der-Chyuan Lou, Chao-Lung Chou , Hung-Yuan Wei , Hui-Feng Huang(2013) "Active steganalysis for interpolation-error based reversible data hiding"

The art of embedding secret data into common digital media, which also conceals the existence of hidden messages is called steganography. It is a very important factor in obtaining tje goal of private communication. There are some essential requirements for steganography such as capacity and imperceptibility.

CLASSIFICATION OF STAGANOGRAPHY :

A. Based on detection capabilities(Chandram ouli, 2003) :

1. Passive Steganalysis : It focuses on revealing the presence of hidden message

2. Active Steganalysis : It aims at estimating some important parameters of the embedding method.

B. Based on objectives of steganalysis(Luo et al. , 2008)

1. Targeted Steganalysis: It is designed for detecting specific Steganographic algorithms.

2. Blind steganalysis : It is designed to detect message independent of the embedding algorithms.

3 Conclusion

Steganography and steganalysis serve as two sides of a coin. One side is the attempt to transmit secret message under multimedia signals and the other is the effort to detect or prevent such hidden communication. Although some effective steganalysis mechanism have been introduced, however there are may tools that can withstand the effectiveness of steganalysis to some extent.

The paper gives review of some effective steganography and steganalysis tools that can be used to detect the hidden original document with in the object. Still, the researchers should make more efforts in the direction of developing new steganalysis tools and techniques to stay a step ahead from the malicious users of Steganography.

4 Acknowledgement

This study was conducted under the supervision of the Ramandeep kaur in partial fulfillment of the requirements of a Master of Technology in Computer Science. I wish to thank Assistant Professor Ramandeep Kaur at Adesh Institute of Engineering and Technology, Faridkot under Punjab Technical University , Jalandhar for her support over the period in which this article was written.

References

[1] Der-Chyuan Lou, Chao-Lung Chou , Hung-Yuan Wei , Hui-Feng Huang(2013) "Active steganalysis for interpolation-error based reversible data hiding"

[2] Lalit Kumar, Vashishtha ,Tanima Dutta Arijit Sur(2013) "Least Significant Bit Matching Steganalysis Based on Feature Analysis"

[3] Fengyong Li, Xinpeng Zhang, Bin Chen, and Guorui Feng(2013) "JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier"

[4] Chunfang Yang, Fenlin Liu, Xiangyang Luo, and Ying Zeng(2012) "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography"

[5] Xikai Xu, Jing Dong, Wei Wang and Tieniu Tan(2013) "video steganalysis based on the constraints of motion vectors"

[6] Xiaolong Li, BinLi, XiangyangLuo, BinYang, Ruihui Zhu (2013) "Steganalysis of a PVD-based content adaptive image steganography"