Review of Various Steganalysis Techniques

Rajwinder Kaur[1], Sandeep Kaur Dhanda[2]

[1]rajwinderbrar45891@gmail.com
[1,2]BBSBCET, Fatehgarh Sahib, Punjab

***Abstract*—Steganography and steganalysis received a great deal of attention from media and law enforcement. Many powerful and robust methods of steganography and steganalysis have been developed. In this paper we are considering the methods of steganalysis that are to be used for this processes. Paper giving some idea about the steganalysis and its method.**

***Keywords*— Steganography, Steganalysis**

I. INTRODUCTION

Steganalysis is used to detect and / or estimate the hidden information from observed data with little or no knowledge about the steganography algorithm. The goal of steganalysis is to collect the ample evidence about the presence of embedded message. The importance of steganalytic techniques is increasing. Steganalysis finds its use in computer forensics, cyber warfare, tracking the criminal activities over the internet.

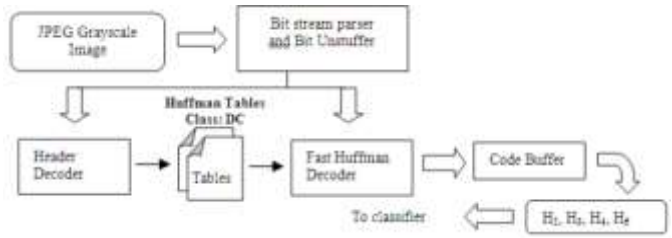

Fig1. Steganalyzer Model Illustrating Huffman Feature Extraction

The aim of steganography is to hide information imperceptibly into a cover, so that the presence of hidden data cannot be diagnosed. Steganalysis aims to expose the presence of hidden data. In this letter, we present ways to detect a simple—but particularly difficult to uncover—embedding method for data in bitmap images; to our knowledge, this is the first reliable detector of its kind.

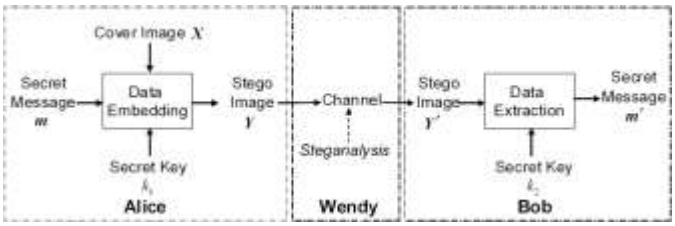

Fig2. The model of steganography and steganalysis

II. RELATED WORK

Much work has been done on steganalyzing LSB steganography in the initial stage of the development of steganalysis. Many steganalytic methods toward LSB steganography have been proved most successful, such as Chi-square statistical attack [2], RS analysis, sample pair analysis (SPA) analysis, weighted stego (WS) analysis, and structural steganalysis etc.

Many other steganalytic techniques [1] have been proposed in recent years. Some steganalytic methods, for example, the Chi-square attack, are effective to LSB steganography for spatial images as well as JPEG images. The fact that LSB steganography is vulnerable to attack implies that high imperceptivity does not guarantee a high security level. The first ever statistical steganalysis was proposed by Westfeld and Pfitzmann [3]. There approach is specific to LSB embedding and is based on powerful first order statistical analysis. It identifies Pairs of Values (POVs) that consist of pixel values, quantized DCT coefficients or palette indices which get mapped to one another on LSB flipping. After the message embedding, the total number of occurrence of two members of certain POV remains the same. This concept of pair wise dependencies is leads to design a statistical Chi-square test to detect the hidden messages [4]. A technique in grayscale images is proposed by Zhang and Ping [5].This technique uses different image histogram as the statistical analysis tool. Measure of the weak correlation between the LSB plane and the rest of the planes is done by the translation coefficients between different image histograms. This algorithm can identify the existence of secret messages embedded using sequential or random LSB replacement in images and also can estimate the amount of secret messages. This algorithm shows a better performance and computation speed than RS analysis method. Benton and Chu [6] proposed a soft computing approach to steganalysis specific to LSB. Decision trees and neural networks are used independently for detection purpose. The features are extracted from images which are based on the variables for estimating the embedding probability in the RS method. This approach different from original RS method. The goal of this method is to decide whether the image contains hidden data but not to estimate the embedding probability. Xiang-dong Chen, et al. [7] a proposed a steganalysis technique based on bit plane randomness tests. Two binary sequences are obtained by scanning the 7th and 8th bit planes of the image with Hilbert scan. The randomness of these two sequences is tested individually by 14 kinds of randomness tests. The results of these tests form a vector and are used to construct a SVM classifier to distinguish stego images from the clean ones. In [8] , Andrew D. Ker , proposed steganalysis methods for extensions of least-significant bit overwriting to both of the

two lowest bit planes in digital images.There are two distinct embedding paradigms. He investigates how detectors for standard LSB replacement can be tailored to such embedding, and how the methods of "structural steganalysis", that gives the most responsive detectors for standard LSB replacement, He also compares the detectability of standard LSB embedding with the two methods of embedding in the lower two bit planes. In paper [9], they described a new very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images. By inspecting the differences in the number of regular and singular groups for the LSB and the "shifted LSB plane", we can reliably detect messages as short as 0.03bpp. In a image, neighbor pixels have a high cross correlation. This is also true for LSB planes of close pixels. Inserting random bits using LSB method alleviates naturally the said correlations. Based on these feature, a method is proposed in [10] to detect LSB stego images by using 2-D autocorrelation coefficients of image. Since matrix of autocorrelation is symmetric, just some of its coefficients are used. These features are applied for classifying the stego image and natural image .The results show that this new method has a high performance, and is more effective than other methods. Jan Kodovský et al. [11], constructed a new quantitative steganalyzers for steganographic techniques which hide data using LSB embedding in quantized DCT coefficients of a JPEG file. They have explored two approaches: change-rate estimation using the maximum likelihood principle with a pre cover model and a heuristic approach based on minimizing a penalty functional obtained from a combined analysis of the embedding operation and properties of natural images. The techniques are applied to Jsteg and its modified version called symmetric Jsteg. Experiments are used to compare the new methods with current state of the art. **H.B.Kekre et al.** [12], proposesd a steganalysis technique for both grayscale and color images. Feature vectors derived from gray level co-occurrence matrix (GLCM) in spatial domain, which is sensitive to data embedding process has been used. Difference between the features of stego and non-stego images is used for steganalysis. Distance measures like Absolute distance and Euclidean distance are used for classification. Experimental results demonstrate that the proposed scheme outperforms the existing steganalysis techniques in attacking LSB steganographic schemes applied to spatial domain. LSB matching steganalysis method detects the existence of secret messages embedded by LSB matching steganography in digital media.LSB matching may be modeled in the context of additive noise independent of the cover image. The result of additive noise steganography to the image histogram is alike to a convolution of the histogram of the cover image and stego-noise PMF. LSB matching more difficult and hard to detect as compared to simple LSB replacement. This study presents a survey of LSB matching steganalysis for digital image. Andew D. Ker et al. proposed a steganalysis technique for LSB matching in [13]. The technique works for grayscale images. It was observed that the down sampling operation affects the center of mass of the HCF of stego image and this variation was used as the discriminator. These techniques produced reliable detectors for LSB matching in grayscale images. But the embedded message length highly affects the results. Q. Liu et al. [14] proposed a scheme for steganalysis of LSB matching steganography .It is based on feature extraction and pattern recognition techniques. The correlation features are extracted for color images.Statistical pattern recognition algorithms are applied to train and classify the feature sets. This scheme is highly efficient for colour images and reasonably efficient for grayscale images. In paper [15] Fangjun Huang, proposes a new technique for attacking the LSB matching based steganography. The least two or more significant bit-planes of the cover image will be changed during the embedding in LSB matching steganography .So the pairs of values do not exist in stego image. In the proposed method, they got an image by combining the least two significant bit-planes and divide it into 3×3 overlapped sub images. The sub images are grouped into four types. Embedding a random sequence by LSB matching and then calculating the alteration rate of the number of elements, they found that the alteration rate is higher in cover image than in the corresponding stego image. Experimental results show that the proposed algorithm is competent to detect the LSB matching stegonagraphy on uncompressed gray scale images. In [16], they expand the LSB matching image steganography and proposed an edge adaptive scheme which can choose the embedding regions according to the size of covert message and the difference between two consecutive pixels in the cover image.The results show that the new scheme can enhance the security significantly compared with typical LSB-based approaches while maintainning higher visual quality of stego images at the same time. Zhihua XIA et al. presented the detection of spatial domain least significant bit (LSB) matching steganography in gray images [17]. Three features, which are based on image histogram, neighborhood degree histogram and run-length histogram, are extracted first. Then, support vector machine is utilized to learn and distinguish the difference of features between cover and stego images. Experimental results show that the proposed method gives reliable detection ability and outperforms the two previous state-of-the-art methods.

III. STEGANALYSIS TECHNIQUE

Steganalysis can be broadly classified into two classes: signature steganalysis and statistical steganalysis. The division is based on whether the signature of the steganography technique or the statistics of image is used to identify the presence of concealed messages in images embedded using steganography.Based on its application fields, it can be further divided into specific methods and universal methods. A specific steganalytic method utilizes the knowledge of a targeted steganographic technique and may only be appropriate to such a kind of steganography. A universal steganalytic method is used to detect several kinds of steganography. Usually universal methods do not require the

knowledge of the embedding operations. Hence, it is also called blind method.

1) **Signature steganalysis** Steganography methods hide secret information and manipulate the images and other digital media in ways as to remain imperceptible to human eye [5]. Steganography alters the media properties due to the insertion of message bits in the form of degradation or repeated patterns, which act as signatures that convey the existence of embedded message [3] . For detecting the existence of hidden message in a suspicious image is to look for these repetitive patterns signatures of a steganography tool .These particular signatures automatically exploit the tool used in embedding the messages. Such methods looks at palette tables in GIF images and any anomalies caused there by common stego tools. When the message is embedded sequentially such attacks give promising results but, are hard to automatize and their reliability is highly doubtful.

2) **Statistical steganalysis** The statistics of an image undergo alterations due to information hiding. Statistical steganalysis analyses the underlying statistics of an image to detect the secret embedded information. Statistical steganalysis is more commanding than signature steganalysis, because mathematical techniques are more responsive than visual perception [3].

2.1) **Specific statistical steganalysis:** These types of techniques are established by analyzing the embedding operation and determining certain image statistics. Such techniques need a detailed knowledge of embedding process. These techniques capitulate very accurate results when used against a target steganography technique. Specific statistical steganalytic tools is used for finding secret message from stego-images embedded by LSB embedding, LSB matching, spread spectrum, JPEG compression and other transform domain [3].

2.2) **Universal statistical steganalysis:** Universal statistical steganalysis comprise the statistical steganalysis method that is not tailored for a specific steganography embedding method. It requires less or even no priori information of the under attack steganographic methods for detection of secret message. It used a learning based strategy which involves training based on cover and stego-images. Neural network, clustering algorithms and other soft computing tools are used to construct the detection model from the experimental data. These techniques do not depend on the behavior of embedding algorithms.

Table 1: Recapitulation of steganalysis approaches[18]

Papers / Characteristics	Neural Network Based Steganalysis in Still Images	Steganalysis Based on Moments of Characteristic Functions Using Wavelet Decomposition, Prediction-Error Image, and NN	Texture based steganalysis
Type of steganalysis	Passive	Passive	Passive
Features	Transform domain includes : DFT, DCT, DWT	Moments of characteristics function, Prediction error-image.	LBP(Local Binary Pattern)
Type of Neural Network	Back-Propagation Neural Networks	Feed forward NN with back-propagation.	Not mentioned
Use of ANNs	For classifying	For classifying	For selecting
Number of data hiding methods	One " Brain Chen's quantization (3)	Five " Cox et al. SS, Piva et. al's blind SS , Huang and Shi's block SS, generic QIM and a generic LSB"	One " Blindside"
Images used	Each image is divided into 8x8 sub-block	1096 sample images included in the CorelDRAW (www.corel.com)	1000 clean color JPG images and 1000 stego-images
Results	Hidden images: 85.4% No hidden images: 75.0%	Five methods combined: 98.7 %	Hidden images: 68.5% No hidden images: 99.1%

IV. STEGANALYSIS TOOLS

There are various steganalytic tools available in market like: PhotoTitle, Benchmark, StirMark and 2Mosaic etc [14]. These steganalytic tools can remove steganographic content from any image. Removal is achieved by destroying secret message by two techniques: – break apart and resample. StegDetect, StegBreak, StegSpy discover information embedded via the following tools - Hiderman,Jsteg-shell, JPhide, and Seek, Camouflage , F5, appendX, , JPHIde and, JPegX. Steganography Analyzer Real-Time Scanner is the best steganalysis software at the moment that can analyze all network traffic to look for traces of steganographic communication.

V. CONCLUSION

Steganalysis is meant to reverse of stegnography in which we have to extract the content of the image by some techniques in which we make an image blurred and upto some extent distortion. This so-called Kerckhoff's principle is always assumed in cryptography Critical review of the current Steganalysis algorithms that is used in the steganalysis technique. This paper gave a clear picture of the current trends in steganalysis. It can be concluded that no single strategy works best. Depending on the amount of statistical information available at hand, a proper choice has to be made.

VI. REFERENCES

[1] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, "A Survey on Image Steganography and Steganalysis," Journal of Information Hiding and Multimedia Signal Processing ,Volume 2, Number 2, April 2011 ,pp.142-172

[2] Souvik Bhattacharyya , Indradip Banerjee and Gautam Sanyal, " A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier," Journal of Global Research in Computer Science, Volume 2, No. 4, April 2011,pp.1-15.

[3] A. Westfeld, A.Pfitzmann, " Attacks on steganographic systems," Proc. of Information Hiding, Third Int. Workshop, Dresden, Germany, September 28–October 1, 1999, pp. 61–75.

[4] N.F. Johnson, S. Jajodia, "Steganalys of images created using current steganography software, in: Lecture Notes in Computer Science," vol. 1525, Springer-Verlag, Berlin, 1998, pp. 273–289.

[5] T. Zhang, X. Ping, "Reliable detection of LSB steganography based on difference image histogram," in: Proc. ICASSP, vol. I, 2003, pp. 545–548.

[6] Ryan Benton, Henry Chu, "Soft computing approach to steganalysis of LSB embedding in digital images," in: 3rd Int. Conf. on Information Technology Research and Education, 27–30 June 2005, pp. 105–109.

[7] Xiang-dong Chen, "Detect LSB steganography with bit plane randomness tests," in: Proc. of 6th World Congress on Intelligent Control and Automation, China, June 21–23, 2006.

[8] Andrew D. Ker ," Steganalysis of Embedding in Two Least-Significant Bits , " Information Forensics and Security, IEEE Transactions on**,** Volume 2 **,** Issue 1, March 2007,pp.46 - 54

[9] Jessica Fridrich, Miroslav Goljan, Rui Du, "Reliable Detection of LSB Steganography in Color and Grayscale Images"

[10] Arezoo Yadollahpour, Hossein Miar Naimi ,"Attack on LSB Steganography in Color and Grayscale Images Using Autocorrelation Coefficients," European Journal of Scientific Research ,ISSN 1450-216X Vol.31 No.2 © EuroJournals Publishing, Inc. 2009, pp.172-183

[11] Jan Kodovský, Jessica Fridrich, "Quantitative Steganalysis of LSB Embedding in JPEG Domain ," MM&Sec'10, September 9–10, 2010, Roma, Italy.

[12] H.B. Kekre, A.A. Athawale & S.A.Patki, " Steganalysis of LSB Embedded Images Using Gray Level Co- Occurrence Matrix," International Journal of Image Processing (IJIP), Volume 5 ,Issue 1: 2011

[13] A.D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett. 12 (6), June 2005,pp. 441–444.

[14] Qingzhong Liu, Andrew H. Sung, Jianyun Xu, Bernardete M. Ribeiro, Image complexity and feature extraction for steganalysis of LSB matching steganography," in: IEEE Int. Conf. on Pattern Recognition, vol. 2, 2006, pp. 267–270.

[15] Fangjun Huang, Bin Li, Jiwu Huang ,"ATTACK LSB MATCHING TEGANOGRAPHY BY COUNTING ALTERATION RATE OF THE NUMBER OF NEIGHBOURHOOD GRAY LEVELS," ©2007 IEEE I - 401 ICIP 2007

[16] Fangjun Huang, Jiwu Huang," Edge Adaptive Image Steganography Based on LSB Matching,"INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS, VOL. 5, NO. 2, JUNE 2010

[17] ZHIHUA XIA, ET AL.,"A LEARNING-BASED STEGANALYTIC METHOD AGAINST LSB ATCHING STEGANOGRAPHY RADIOENGINEERING," VOL. 20, NO. 1, APRIL 2011,pp102-109

[18] NOUHA KOBSI, HAYET FARIDA MEROUANI, "Neural Network Based Image Steganalysis: A Comparative Study",