Review of Various Steganalysis Techniques

Ajayta Sabharwal
Indo Global Colleges of Engineering, Punjab Technical University, Punjab, India
ajaytasabharwal@gmail.com

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 these processes. This paper gives some idea about the steganalysis and its method.

Keywords—Steganalysis, Detecting hidden information, Steganalytic techniques, Steganalysis tools.

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 steganalysis techniques is increasing. Steganalysis find its use in computer forensics, cyber warfare, tracking the criminal activities over the internet.

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 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 is 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] 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 an 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 Kodovsky 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], proposed 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. Andrew 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
Steganography methods hide secret information and manipulate the images and other digital media in ways so 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 thereby 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].

a) **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 steganalysis 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].

b) **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 prior 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]

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

IV. STEGANALYSIS TOOLS

There are various steganalysis tools available in market like: Photo Title, Benchmark, StirMark and 2 Mosaic 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, appendixX, , 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 steganography 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.

REFERENCES


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

© www.ijarcsse.com, All Rights Reserved