



Approaches and Methods for Steganalysis – A Survey

L. Rathika¹, B. Loganathan²

M. Phil Scholar, Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu¹

Associate Professor, Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu²

Abstract: Information security is the main concern of current scenario, which has a number of approaches to preserve data via cryptography, watermarking, steganography techniques. One such approach may always create a negative impact on all the process, which involves with vulnerable activities such as malicious and harmful content spreading by embedding. To identify such content, steganalysis has been performed. The counter technique of image steganography is called as image steganalysis, which begins by recognizing the object that exists in the embedded source file. This paper gives a survey of the approaches and techniques, tools used in steganalysis. This paper also makes the discussion about the problems of those techniques in the real-time analysis.

Keywords: Data security, Steganalysis, Steganography, Image Processing, Pixel-Decimation.

I. INTRODUCTION

Secret data sharing and secure communication is the major research area, which linked with several security applications. This type of secret data sharing is popular with the help of steganography approaches to deliver safely over computer networks without interference. Steganography is a technique that hides data among the bits of a cover file such as audio, video and image files [1]. In steganography the existence of a message is often unknown. Both data embedding and extraction need a digital image processing technique to deploy. The application such as medical safety, terrorism and hacking types of application need steganalysis. Steganalysis provides a way of detecting the presence of hidden information from the embedded content. This paper provides an overview and comparative analysis of different Steganalysis approaches.

A. Image steganography:

Image steganography is defined as the covert embedding of data into digital pictures. Though steganography hides information in any one of the digital Medias, digital images are the most popular as carrier due to their frequency usage on the internet [2]. Because the size of the image file is huge in size, it can cover large amount of information. The Human Visual System cannot differentiate the normal image and the image with hidden data easily. The digital images are usually contains large amount of redundant bits in nature, where images are became the most popular cover objects for steganography. So every research uses image as cover file with different image formats such as JPEG, BMP, TIFF, PNG or GIF files can be used as cover objects to deploy steganography. A bitmap or BMP format is a simple image file format. Data is easy to manipulate, since it is uncompressed. But the uncompressed data leads to larger file size than the compressed image. JPEG (Joint Photographic Expert Group) is the most commonly used image file format. It uses lossy compression technique; the quality of the image is excellent. The size of the file is also smaller. TIFF format uses lossless compression. The file is reduced without affecting the image quality. GIF (Graphics Interchange format) has color palette to provide an indexed colors image. It uses lossless compression and it can store only 256 different colors, it is not suitable for representing complex photography with continuous tones, PNG (Portable Network Graphics) file format provides better colors support, best compression, and gamma correction in brightness control and image transparency. PNG format can be used as an alternative to GIF to represent web images.

B. Image Steganalysis:

Steganography is a strong technique to hide a secure message, however, it also vulnerable when the technique used to spread malicious and harmful content by embedding. To identify such content, staganalysis has been performed. The counter technique of image steganography is known as image steganalysis, which begins by recognizing the object that exists in the embedded source file. The aim of this process is not to advocate the removal or disabling of valid hidden information such as copyrights, but to point out approaches that are vulnerable and may be exploited to investigate illegal and dishonest hidden information [3].

Security threats analysis on hidden information may take several forms like detecting, extracting, and disabling or destroying hidden information [4]. An attacker may also embed contradict information over the existing hidden data.



These approaches vary depending upon the methods used to embed the information into the cover media. Some amount of changes and degradation may occur to carriers even though such distortions cannot be detected easily by the human perceptible system. The alteration or changes on the carrier image may be anomalous to the normal carrier. This will be discovered the tip about the hidden information to the user. Numerous tools exist in performing steganography process, and they vary in their approaches and steps for hiding information over different types of carrier media. Finding hidden content is very complex without knowing the tool an key used in that. Some of the steganographic approaches have characteristics that act as signatures for the method or tool used.

The objective of steganalysis is to perceive the hidden information. This method exploits the various image processing techniques such as cropping, filtering etc. Passive steganalysis simply corrupt the image if any suspicion arises. Active steganalysis attempts to find the algorithm to hide the information and tried to retrieve the message. Algorithms like sample pair analysis; RS analysis can detect LSB substitution stego systems. Chi square analysis is based on statistical distribution of ones and zeros in an image. This particular characteristic can determine whether the image intensities follow any distributed pattern or random pattern. In general, steganalysis is classified into visual steganalysis, structural steganalysis, statistical steganalysis and learning steganalysis. Visual and structural steganalysis are well suited for manual inspection, and visual steganalysis completely depends on a subjective interpretation of visual data. Statistical and learning steganalysis are well suited for automated calculation.

C. Applications of Steganalysis:

- Medical safety: Current image formats such as Digital Imaging and Communications in Medicine separate image data from the text like such as patients name, date and physician details along with the result that the link between image and patient occasionally gets mangled by protocol converters. Thus embedding the patient's name in the image could be a useful safety measure [5].
- Terrorism: According to government officials terrorists use to hide maps and photographs of terrorist targets and giving instructions for terrorist targets.
- Hacking: The hacker hides a monitoring too, server behind any image or audio or text file and shares it with mail or chat which will get installed and executed which will help the hacker to do anything with the workstation.

D. Steganalysis Methods

Steganalysis is the method, which detects the presence of hidden data; this process can be categorized by different types such as Statistical steganalysis which contains spatial domain. Transform domain and Feature based steganalysis. The Statistical steganalysis helps to detect the existence of the hidden message, statistical analysis is done with the pixels and it is further classified as spatial domain steganalysis and transforms domain steganalysis. In spatial domain, the pair of pixels is considered and the difference between them is calculated. The pair may be any two neighboring pixels. They may be selected within a block otherwise across the two blocks. Finally the histogram is plotted that shows the existence of the hidden message. In transform domain, frequency counts of co-efficients are calculated and then histogram analysis will be performed at the time of steganalysis. With the help of this, the cover and stego images can be differentiated. However, this method is not providing information about the embedding algorithms. To overcome this problem, we may choose feature based steganalysis. The staganalysis methods are shown in fig 1.0.

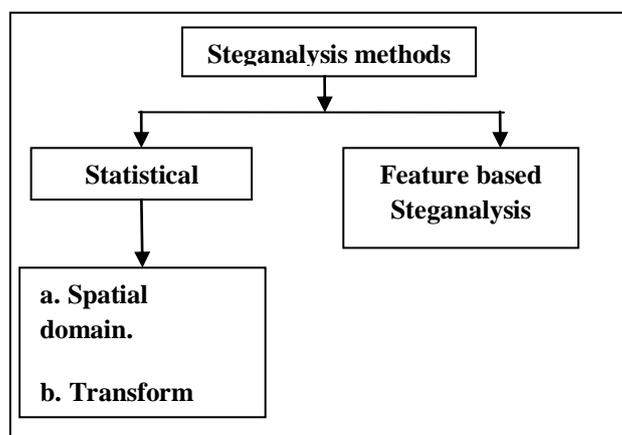


Fig 1.0 Steganalysis methods

In the Feature based steganalysis approach, the features of the given image will be obtained for selecting and retaining relevant information from the cover image. These extracted features are used to detect hidden message in an image. They can also be used to train classifiers.



E. Classification of steganalysis

There are certain types of algorithms available in the literature to perform classification; the classification is a supervised process where it needs a prior training to classify the data into normal or stego data. The steganalysis algorithm may or may not depend on the steganographic algorithm (SA). Based on this, steganalysis is classified as Specific and generic algorithms. Few algorithms depend on the steganographic algorithms and few not.

1. Specific / Target steganalysis.
2. Generic / Blind / Universal steganalysis.

1. Specific steganalysis: The SA is known and the designing of detector (steganalysis algorithm) is based on SA. The steganalysis algorithm is dependent on the SA. This type of steganalysis is based on analyzing the statistical properties of an image that change after embedding. The advantage of using specific steganalysis is the results are very accurate. The specific or target steganalysis are very limited to particular embedding algorithm. So it is not fully applicable for all types of algorithms. And it also not supports all image formats.

2. Blind / Universal steganalysis: In universal method, the steganalysis algorithm is not recognized by all. Therefore, anyone can design a detector to detect the presence of the secret message that will not depend on steganalysis algorithms. Comparing with specific steganalysis, universal is common and less efficient. Still universal steganalysis is widely used than specific one because it is independent of the SA. This research focuses on universal steganalysis. It includes the following 2 phases like feature extraction from the data and classifying them into two distinct groups.

- a. Feature Extraction.
- b. Classification.

a. Feature Extraction: It is a process of creating a set of distinct statistical attributes of an image. These attributes are known as feature. Feature Extraction is nothing but a dimensionality reduction. The extracted features must be sensitive to the embedding objects and the Image quality metrics and also 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.

b. Classification: It is a way of categorizing the images into classes depending on their feature values. Supervised learning is one of the primary classifications in steganalysis. Supervised learning allows learning under some supervision. In this learning, a set of training inputs that includes input features is given as input to train the classifier. After the training, class label is predicted based on the features that are given. Steganalysis use the following classifiers:

1. Multivariate regression.
2. Fisher linear discriminant (FLD).
3. Support vector machine (SVM).
4. Artificial neural network (ANN).

1. Multivariate regression: It consists of regression co-efficient. In the training phase, regression coefficients are predicted using minimum mean square error. This algorithm is effective when the training samples are valid and huge.

2. FLD: It is a linear combination of features which maximizes the separations. In the classification method, multi dimensional features are projected into a linear space. Using this algorithm, the feature extraction and matching will be performed effectively, because it uses the linear method at the time of feature extraction and content extraction.

3. SVM: Support Vector Machine is a popular supervised learning process algorithm, which learns from the given sample i.e. training dataset. This algorithm is trained to recognize and assign class labels based on a given set of features and objects. In general, SVM creates a hyper plane selection problem and may arise outliers.

4. ANN: It is defined as an information processing model that simulates biological neuron approaches and it includes several steps to classify the data. Feed forward and back propagation neural networks are commonly used in classification. The classification process has 2 steps, training and testing. In a training phase, the neural network associates the outputs with the given input patterns, by modifying the weights of inputs. In a testing phase, the input pattern is identified and the associated output is determined. This thesis uses ANN classifier for detecting the presence of hidden information.

Steganalysis tools

Steganalysis usually consist several processes like cropping, blurring, image resizing, noise removal and compression process. Various steganalysis tools are available to detect the presence of hidden information with the stego image. And few tools only provide the above process. Some of the steganalysis tools are mentioned below:



1. StegDetect.
2. StegSecret.
3. JPSeek.
4. StegBreak.

StegDetect: This software is an automated tool for detecting steganographic content in images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images. This software will run on the linux platform. Currently, the detectable schemes are jsteg, jphide, invisible secrets; OutGuess 01.3b, F5, appendX, and camouflage. Using linear discriminant analysis, it also supports detection of new stego systems. The main drawback of this software is it works only for JPEG images. Currently, there is no support for parameter training. The only exported knob is the sensitivity level. Future versions will export all detection parameters via a configuration file.

JPSeek: It is a program that allows detecting the hidden message inside a jpeg image. There are various versions of similar programs available on the internet but JPSeek is rather special. The design objective is same as JPHide.

StegSecret: StegSecret software aim is to gather, to implement and to make easier the usage of steganalysis techniques, especially in digital media such as images, audio and video. This software warns about the insecurity of several steganographic tools and steganographic algorithms available in Internet. It is a steganalysis open source project that makes possible the detection of hidden information in different digital media. StegSecret is java-based multiplatform steganalysis tool that allows the detection of hidden information by using the most known steganographic methods. It detects EOF, LSB, and DCT like techniques.

StegBreak: It launches brute-force dictionary attacks on JPG image. The StegBreak states a brute-force dictionary attack against the specified JPG images. And while comparing with the other tools, this is effectively work on JPG image formats.

Other steganalysis tools: Some more image steganalysis tools are 2Mosaic, StirMark Benchmark, Phototile, StegSpy, Stego Suite, Steganalysis Analyzer Real-Time Scanner, JSteg detection, JPHide detection, OutGuess detection.

II. LITERATURE REVIEW

The visual attacks (Westfeld et al. [6]) detect the steganography by making use of the ability of human eyes to inspect the images for the corruption caused by the embedding. Pairs analysis was proposed (Fridrich et al. [7]). This approach is well suited for the embedding archetype that randomly embeds messages in LSBs of indices to palette colors of palette image.

The F5 algorithm was introduced by German researchers (Westfeld [8]). It embeds message bits into non-zero AC coefficients and adopts matrix encoding to achieve the minimal number of changes in quantized coefficients during embedding process. The matrix encoding is the core of the F5 algorithm. It is determined by the message length and the number of non-zero AC coefficients. It can be represented as the form (P Q, and R). The parameter P tells how many coefficients at most will be modified during embedding, and Q is the number of coefficients involved in embedding the k-bit message. In the embedding process, the message is divided into segments of R bits to embed into a group of n randomly chosen coefficients. F5 algorithm manipulates the quantized co-efficient when the hash of that group does not match the message bits, thus the histogram values of DCT co-efficient are modified. For example, if the shrinkage occurs, the number of zero AC coefficients will increase and the number of remaining non-zero coefficients decreases with embedding. The changes in the histogram of DCT co-efficient may be utilized to detect the presence of hidden message.

Fridrich et al. [9] developed a steganalytic technique based on this process for detection of LSB embedding in color and grayscale images. They analyze the capacity for embedding lossless data in LSBs. Randomizing the LSBs decreases this capacity. To examine an image, they define Regular groups (G) and Singular groups (H) of pixels depending upon some properties. Then with the help of relative frequencies of these groups in the given image, in the image obtained from the original image with LSBs flipped and an image obtained by randomizing LSBs of the original image, they try to predict the levels of embedding. Many steganalysis researchers such as Neil et al. [10] attempt to categorize steganalysis attacks to recover modify or remove the message, based on information available. The steganalysis technique developed can detect several variants of spread-spectrum data hiding techniques (Marvel et al. [11]). The first steganalysis technique using wavelet decomposition was developed by Farid [12] have shown that this change is proportional to the level of embedding. They also showed that, if an image is cropped by 4 rows and 4 columns, then original DCT histogram can be obtained. The basic assumption here is that the quantized DCT coefficients are robust to small distortions and after cropping the newly calculated DCT coefficients will not exhibit clusters due to quantization.



Also, because the cropped stego image is visually similar to the cover image, many macroscopic characteristics of cover image will be approximately image and comparing with that of a stegoed image, the hidden message length can be calculated. Sullivan et al. [13] use an empirical matrix as the feature set to construct a steganalysis. Chen et al. [14] improved and applied the statistical moments on JPEG image steganalysis with enriched features.

The previous methods in literature used to detect LSB hiding is the 2 chi-squared techniques. And this technique later successfully used to stegdetect tool for steganalysis. This effectively detects of LSB hiding in JPEG coefficients. A different LSB detection scheme later was proposed by (Avcibas et al. [15]). This used binary similarity measures between the 7th bit plane and the 8th (least significant) bit plane sequentially. It is assumed that there is a natural correlation between the bit planes that is disrupted by LSB hiding. This scheme does not auto regulate on a per image basis and instead calibrates on a training set of cover and stego images. The scheme works better than a generic steganalysis scheme, but not as well as state-of-the-art LSB steganalysis. Later, a new approach with earlier LSB is developed and declared as a stego detection scheme. This utilizes binary similarity measures between the 7th bit plane and the 8th (least significant) bit plane. It is assumed that there is a natural correlation between the bit planes that is disrupted by LSB hiding. This scheme does not auto-calibrate on a per image basis, and instead calibrates on a training set of cover and stego images. The scheme works better than a generic steganalysis scheme, but not as well as state-of-the-art LSB steganalysis.

Scheme, proposed by Fridrich et al. [16] is a specific steganalysis method for detecting LSB data hiding in images. Sample pair analysis is a more rigorous analysis due to (Dumitrescu et al. [17]) of the basis of the RS method, explaining why and when it works. Miche et al. [18] uses estimates of the joint probability mass function (PMF) to increase the detection rate of RS/sample pair analysis. Author's uses local estimators based on pixel neighborhoods to slightly improve LSB detection over RS.

It is exposed for typical cover distributions that the expected value or center of mass of the existing HCF scheme. This scheme does not increase the size after hiding. So this is considered as a best stegano approach. But, the performance in practice typically decreases the quality of the image. The authors choose then to use the technique as a feature to train a Bayesian-multivariate classifier to discriminate between cover and stego information's. The authors performed tests on RGB images by applying a combined COM of each color plane, with reasonable success in detecting additive hiding.

Fridrich et al. [19] content-independent stochastic modulation is statistically identical to spread spectrum and Celik et al. [20] proposed using rate-distortion curves for detection of LSB hiding. They observe that data embedding typically increases the image entropy, while attempting to avoid introducing perceptual distortion to the image. On the other hand, compression is designed to reduce the entropy of an image while also not inducing any perceptual changes. It is expected therefore that the difference between a stego image and its compressed version is greater than the difference between a cover and its compressed form. Distortion metrics such as MSE mean absolute error and weighted MSE. These techniques are used to measure the difference between an image and compressed version of the image. A feature vector consisting of these distortion metrics for several different compression rates (using JPEG2000) is used to train a classifier. False alarm and missed detection rates are each about 18%.

III. CONCLUSION

The steganalysis plays an important role in the current trend. Detection and analysis of steganographic images are the most important process in several real-time applications. The lack of training samples for steganalysis make these processes much complicated. This steganalysis process can be performed by effective classification and image processing techniques and approaches. In this paper, we reviewed several different methods to achieve effective steganalysis on different steganographic techniques. This survey presents various techniques of the steganalysis approach to solving the security problem. From the analysis, we discover an optimal and effective algorithm and technique to handle steganographic dataset.

REFERENCES

- [1]. Artz, Donovan. "Digital steganography: hiding data within data." IEEE Internet computing 5.3 (2001): 75-80.
- [2]. Cheddad, Abbas, et al. "Digital image steganography: Survey and analysis of current methods." Signal processing 90.3 (2010): 727-752.
- [3]. Li, Bin, et al. "A survey on image steganography and steganalysis." Journal of Information Hiding and Multimedia Signal Processing 2.2 (2011): 142-172.
- [4]. Chandramouli, Rajarathnam, Mehdi Kharrazi, and Nasir Memon. "Image steganography and steganalysis: Concepts and practice." International Workshop on Digital Watermarking. Springer, Berlin, Heidelberg, 2003.
- [5]. Sullivan, Kenneth, et al. "Steganalysis for Markov cover data with applications to images." IEEE Transactions on Information Forensics and Security 1.2 (2006): 275-287.
- [6]. Westfeld, Andreas, and Andreas Pfitzmann. "Attacks on steganographic systems." International workshop on information hiding. Springer, Berlin, Heidelberg, 1999.
- [7]. Fridrich, Jessica, and Miroslav Goljan. "Practical steganalysis of digital images-state of the art." Proceedings of SPIE. Vol. 4675. 2002.
- [8]. Westfeld, Andreas. "F5—a steganographic algorithm." Information hiding. Springer Berlin/Heidelberg, 2001.



- [9]. Kodovsky, Jan, and Jessica Fridrich. "Quantitative structural steganalysis of Jsteg." *IEEE Transactions on Information Forensics and Security* 5.4 (2010): 681-693.
- [10]. Neil, F. Johnson, and Sushhil Jajodia. "Steganalysis The Investigation of Hidden Information." *Proceedings of the IEEE Information Technology Conference*. 1998.
- [11]. Marvel, Lisa, Brian Henz, and Charles Boncelet. "A performance study of ± 1 steganalysis employing a realistic operating scenario." *Military Communications Conference, 2007. MILCOM 2007. IEEE. IEEE, 2007*.
- [12]. Lyu, Siwei, and Hany Farid. "Steganalysis using higher-order image statistics." *IEEE transactions on Information Forensics and Security* 1.1 (2006): 111-119.
- [13]. Sullivan, Kenneth, et al. "Steganalysis for Markov cover data with applications to images." *IEEE Transactions on Information Forensics and Security* 1.2 (2006): 275-287.
- [14]. Chen, Chunhua, and Yun Q. Shi. "JPEG image steganalysis utilizing both intrablock and interblock correlations." *Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on. IEEE, 2008*.
- [15]. Avcibas, Ismail, Nasir Memon, and Bülent Sankur. "Steganalysis using image quality metrics." *IEEE transactions on Image Processing* 12.2 (2003): 221-229.
- [16]. Fridrich, Jiri, and M. Long. "Steganalysis of LSB encoding in color images." *Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on. Vol. 3. IEEE, 2000*.
- [17]. Dumitrescu, Sorina, Xiaolin Wu, and Nasir Memon. "On steganalysis of random LSB embedding in continuous-tone images." *Image Processing. 2002. Proceedings. 2002 International Conference on. Vol. 3. IEEE, 2002*.
- [18]. Miche, Yoan, et al. "A feature selection methodology for steganalysis." *International Workshop on Multimedia Content Representation, Classification and Security. Springer Berlin Heidelberg, 2006*.
- [19]. Fridrich, Jessica, and Miroslav Goljan. "Digital image steganography using stochastic modulation." *Proceedings of SPIE. Vol. 5020. 2003*.
- [20]. Celik, Mehmet U., Gaurav Sharma, and A. Murat Tekalp. "Universal image steganalysis using rate-distortion curves." *Proceedings of SPIE. Vol. 5306. 2004*.