International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.1., 2016
(Jan-Feb)

REVIEW ARTICLE

ISSN: 2321-7758

A SURVEY OF STEGANALYSIS TECHNIQUES

SONAM CHHIKARA
Jawaharlal Nehru University, New Delhi, India

SONAM CHHIKARA

ABSTRACT

Steganalysis and steganography are two term used for security purpose for embedding and extracting information in media files in imperceptible way. Steganography is the art of secret communication and steganalysis is the art of detecting the hidden messages embedded in digital media using steganography. Many powerful and robust methods of steganography and steganalysis have been introduced in the literature. In this paper, we will discuss various steganalysis techniques used recently for detection of hidden data embedded in media using various steganography techniques.

Key Words— Steganalysis, Steganography, Classifiers, LSB.

I. INTRODUCTION

This is a world of computer and internet and most of the communication is done through internet only. But there are always a chance of attack which interrupt the communication between two parties, this breaks the security of the users and brings the security issue. There are many way of providing security, one of them is steganography. Steganography is an art of hiding the secret data in multimedia files like images, videos, audio etc. Steganography has its Greek origin and means conceal writing where “stega” means “covered” from Greek word steganos and “nography” means “writing” from Greek word graphia. The process of steganography starts by identifying the cover image and the information which is to hidden. This is an ancient art but digital technology gives it new direction so that it can hide information in digital images and signals.

There are many aspects of security during communication like cryptography, watermarking and steganography. All these are different from each other in their terms. First one is cryptography, Cryptography scrambles the message so that it can’t be understood by the third party in between the transmission of message from sender to receiver. This is one of the ancient technique of transferring information overt some untrusted medium but cryptography techniques are more prone to attacks because the cipher text is in unreadable form so anyone can detect that the given data must have something confidential so anyone can try their method to decrypt the code and get some information from it or change that code such that receiver unable to decrypt it. Second method for secure transmission is Watermarking, Watermarking is a process of hiding information within any digital medium like image, audio, video or in any object. Watermarking takes the advantage of imperceptibility of human between two closely related things but there are many detectors or software which can easily detect the watermark data from the digital media. Due to this problem in watermarking techniques another art come into existence i.e, Steganography. steganography hides the information into another information in such a way that presence of the hidden message is not known by anyone. In steganography, there is "cover media which result in "stego media" after hiding information into it. We can combine cryptography and steganography technique for more secure and private communication as it will be more difficult for the steganalyst to find out the encrypted hidden message from the stego media instead of finding out plain message from it. But form the last few years steganography is used more by criminals for sending their important detail, So various steganalysis technique has been introduced for different steganography schemes.

Steganalysis [3,4] is an inverse process of steganography for detecting secret messages hidden using steganography technique. The aim of steganalysis is to find some change in the stego file either there may be change in size of file or statistic of the file may be different or some visible changes. In this way we fails that steganography technique by particular steganalysis technique. The importance of steganalytic techniques that can reliably detect the presence of hidden information in images is increasing. Steganalysis finds its use in computer forensics, cyber warfare, tracking the criminal activities over the internet and gathering evidence for investigations particularly in case of anti-social elements . Apart from its law enforcement and anti-social significance steganalysis also has a peaceful application—improving the security of steganographic tools by evaluating and identifying their weaknesses. .

This paper consists of 4 sections. In Section II, the types of steganalytic techniques will be discussed. Section III , Literature Review on steganalysis technique will be given and then conclusions drawn from the study have been given in Section IV.

II. Types Of Steganalysis

Steganalysis is classified into : Statistical Steganalysis and Signature Steganaysis[5].

1.) Statistical Steganalysis: When secret data hides in an image then the statistics of an image undergo alteration due to information hiding. Analyses this underlying statistics of an image to detect the secretly embedded information. Statistical steganalysis is further divided into specific and universal statistical steganalysis.

1.1) Specific Statistical steganalysis: Specific statistical steganalysis includes the statistical steganalysis techniques that target a specific steganography embedding technique or its slight variation:

- LSB embedding.
- LSB matching.
- JPEG compression.
- Transformation domain, etc.

1.2) Universal Statistical Steganalysis: Universal statistical steganalysis includes the statistical steganalysis techniques that are not tailored for a specific steganography embedding technique. The trick is to find out appropriate sensitive statistical quantities with 'distinguishing' capabilities. A Neural network, clustering algorithms and other soft computing tools are then used to construct the detection model from the experimental data.

2.) Signature Steganalysis: Steganography methods hide secret information and manipulate the images and other digital media in ways as to remain imperceptible to the human eye. But hiding information within any electronic media using steganography requires alterations of the media properties that may introduce some form of degradation or unusual characteristics and patterns. These patterns and characteristics may act as signatures[6] that broadcast the existence of embedded message. Signature Steganalysis is also further divide into Specific and Universal steganalysis.

2.1) Specific Signature Steganalysis: Signatures specific to steganographic tool were used to expose the possibility of hidden information. These specific signatures automatically exploit the tool used in embedding the messages. For eg. Jpegx, a data insertion steganography stool, inserts the secret message at the end of JPEG files marker and adds a fixed signature of the program before the secret message. The signature is the following hex code: 5B 3B 31 53 00. The presence of this signature automatically implies that the image contains a secret message embedded essentially using Jpegx.

2.2) Universal Signature Steganalysis: This technique is not related to the particular steganographic tool. This is used universally, for eg: It has been shown that cover images stored in the JPEG format are a very poor choice for steganographic methods that work in the spatial domain. This is because the quantization introduced by JPEG compression serves as a unique fingerprint that can be used for detections of very small modifications of the cover image.

III. Related WORKS

There is a lot of work has been already done in steganography and steganalysis is also a topic of interest so that steganography techniques can be improved and more secured for successful transmission of secret data. This section includes some steganalysis techniques which are designed for different steganography schemes.

Reliable Detection Of LSB Steganography based on the translation coefficients between difference image histogram[7]. Translation coefficients are defined as a measure of the weak correlation between the least significant bit (LSB) plane and the remained bit planes, and then used to construct a classifier to discriminate the stego-image from the carrier image. This technique is used for detection of the message as well as amount or information hidden in the image. Its performance is better then RS analysis and good computation speed.

Stochastic Approach For Message Length Estimation in ±k Embedding Steganography[8] is proposed for estimation of the number of embedding changes for non-adaptive ±k embedding in images. The secret message is estimated from the stego image using a denoising filter in the wavelet domain. Then the message is further analyzed using ML/MAP estimators to identify the pixels that were modified during embedding.This approach can estimate the message length for very small value of K , i.e , for k=2.This technique can be used for both grayscale and color images. The performance of the method improves with increasing amplitude of the stego signal.

Next technique[9], is an improved version of a blind steganalysis method proposed by Holotyak et al[10]. And compare it to current state-of-the-art blind steganalyzers. The features for the blind classifier are calculated in the wavelet domain as higher-order absolute moments of the noise residual. This technique uses absolute non normalized moments of order 1 to 9. We call this method Wavelet Absolute Moment steganalysis (WAM). This steganalyzer is used for detection of embedding in raster image formats and compared its performance to four previously proposed blind steganalyzers, side information plays an important role in this steganalyzer.

Blind Image Steganalysis Based On Run-Length Histogram Analysis [11] is a simple and effective method proposed based on Run-Length Histogram. This paper focuses on extracting sensitive features to embedding modification , Statistical moments of characteristic functions of image run-length histogram and its variants are taken as features. SVM is utilized as classifier. The first three moments of the CF of three image RLHs are selected as features to distinguish the plain cover image from stego images. This method has a better performance to an untrained stego-algorithm compared to others. Proposed 36-D feature vector provides clearly better detection accuracy compared with 78-D feature vector and the 108-D feature vector.

A Markov Process Based Approach to Effective Attacking JPEG Steganography[12] is proposed steganalysis scheme to effectively detect the advanced JPEG steganography. In this JPEG 2-D array is formed from magnitudes of quantized block DCT coefficients. Markov process is applied to modeling difference JPEG 2-D arrays so as to utilize the second order statistics for steganalysis and a thresholding technique is developed to greatly reduce the dimensionality of transition probability matrices, thus making the computational complexity of the proposed scheme manageable. The proposed scheme has outperformed the existing steganalyzers in attacking Outguess, F5, and MB1.

Next scheme, is improved approach for Steganalysis for JPEG images [13]. In this approach, the Markov approach is expanded to inter-blocks of the DCT domain and to the wavelet domain, additional features on the joint distributions in the DCT domain and the wavelet domain are also designed as well as the features of a polynomial fitting on the histogram of the DCT coefficients. All these features including expanded Markov transition features are called ExPanded Features (EPF). The difference between the original EPF features and the reference EPF features is calculated, and the original EPF features and the difference features are merged together. Then the feature selection methods of support vector machine recursive feature elimination (SVM-RFE) and multi-class support vector machine recursive feature elimination (MSVM-RFE) are utilized to select features for binary classification and multi-class classification, respectively. This new approach successfully improves the steganalysis performance on several JPEG-based steganographic systems, including JPWIN, F5, CryptoBola, Steghide and Model based steganography.

Steganalysis by Subtractive Pixel Adjacency Matrix (SPM)[14] is a novel approach to steganalysis of various embedding methods by utilizing the fact that the noise component of typical digital media exhibits short range dependences while the stego noise is an independent random component typically not found in digital media. The local dependences between differences of neighboring cover elements are modeled as a Markov chain, whose empirical probability transition matrix is taken as a feature vector for steganalysis. Although the SPAM features were primarily developed for blind steganalysis in the spatial domain, it is worth to investigate their potential to detect steganographic algorithms hiding in transform domains, such as the block DCT domain of JPEG. SPM give better performance than WAM.

Steganalysis For Palette-Based Images [15], is a proposed algorithm for GIF images. . In order to capture the dependencies between adjacent colors, two efficient measurements are introduced. First, three generalized difference images between adjacent colors in horizontal, vertical and diagonal directions are constructed. And then, the first-, second- and third-order absolute moments of the characteristic function of three generalized difference images' histograms are extracted. Second, a new feature called color correlogram that can distill the spatial correlation of colors is used to measure the dependencies of neighbor colors. Two-class SVM is used to distinguish the features between the cover images and stego images. Experiments on several current steganography algorithms for GIF images indicate that the proposed features are effective. For some algorithms, the classification accuracy is higher than 80% when the embedding rate is not less than 20%.

Next , a novel approach based on approximate run length [16] is proposed for image splicing detection. This scheme first defined approximate run length, which helps achieve higher performance. SVM is used to classify authentic and spliced images, which constructs features by applying the approximate run length on the original source image, its predict-error image, and DWT based reconstructed images. Compared with other methods, proposed approach can achieve a relatively high detection accuracy with far less computational complexity and much fewer features.

Next approach is Steganalysis of HMPD reversible data hiding scheme [17]. HMPD reversible data hiding scheme involves the modification of pixel differences, which introduces artifacts into the pixel difference histograms. Four-way pixel difference features are used to design a specific steganalysis method for detecting HMPD reversible data hiding scheme. Two-class SVM classifier is used to distinguish stego-images from the cover images with an overall accuracy of 98.51%. The SVM classifier is trained with feature sets extracted from 1785 cover images and 10,710 stego-images with different hiding level (binary tree L= 0 to 5). Using a multiclass SVM classifier, an estimator which is capable of estimating the secret key (hiding level) with an accuracy of 99.77% is designed.

Ensemble Classifiers[18] for Steganalysis of Digital Media are built by fusing decisions of weak and unstable base learners implemented as the

Fisher Linear Discriminant. The training complexity of the ensemble scales much more favorably allowing the steganalyst to work with high-dimensional feature spaces and large training sets, removing thus the limitations imposed by the available computing resources that have often curbed the detector design like SVM in the past. The ensemble is especially useful for fast feature development when attacking a new scheme. Performance wise, ensemble classifiers offer accuracy comparable and often even better to the much more complex SVMs at a fraction of the computational cost.

Rich Model for Steganalysis of Digital Images [19] is proposed for building steganography detectors for digital images. The submodels consider various types of relationships among neighboring samples of noise residuals obtained by linear and non-linear filters with compact supports. The rich model is assembled as part of the training process and is driven by the available examples of cover and stego images. The proposed framework demonstrated on three steganographic algorithms: HUGO, edge adaptive algorithm by Luo et al., and optimally coded ternary ±1 embedding. For these models G-SVM is trained for all three algorithms. The running time of a G-SVM classifier with 3,300-dimensional features, however, was on average 30–90 times higher than the running time of the ensemble classifier with 12,753-dimensional features. The proposed scheme is a step towards automatizing steganalysis to facilitate fast development of accurate detectors for new steganographic schemes. Rich models provide a good general-purpose model for various applications in forensics and in universal blind steganalysis.

Active steganalysis for histogram-shifting based reversible data hiding technique [20] analyzes the characteristics of histogram changing during the data embedding procedure, and then models these features into reference templates by using a 1 ×4 sliding window and then use the combinatorial similarity measure to train the classifier. The proposed steganalysis algorithm is mainly composed of four parts: features extraction, classifier training, stego-images detection and embedding locations estimation. Experimental results show that the proposed algorithm is highly effective on stego-images detection and embedding locations estimation at low bit rates.

TABLE I: COMPARISON OF SOME STEGANALYSIS TECHNIQUES

TECHNIQUE	PROBLEMS	PERFORMANCE
Detection Of LSB Steganography based on the translation coefficients between difference image histogram.[7]	Not good for images stored in JPEG format.	Better than RS analysis for lossless compressed images.
Stochastic Approach For Message Length Estimation in ±k Embedding Steganography.[8]	Not work with noisy cover images such as never compressed images and scans.	Estimate the message length for very small value of k, i.e k=1,2.
Wavelet Absolute Moment steganalysis (WAM).[9]	Totally based on side information given with image.	Used for detection of messages in raster image formats with better performance.
Steganalysis Based On Run-Length Histogram Analysis.[11]	Not work for embedding rate < 0.15 bpp for untrained stego algorithms.	better detection accuracy compared with 78-D feature vector and the 108-D feature vector.
A markov process based approach for JPEG images.[12]	- - -	Work successfully.
Markov approach extension for Steganalysis for JPEG images.[13]	Detection performance decreases when message length is 50% of carrier capacity.	Improves the steganalysis performance on several JPEG-based steganographic systems.

Steganalysis by Subtractive Pixel Adjacency Matrix (SPM).[14]	Less accurate than steganalyzer that uses merged features.	SPM give better performance than WAM.
Steganalysis For Palette-Based Images.[15]	• Not effective for adaptive steganography. • Not consider cartoon & computer generated images.	Accuracy is higher than 80% for embedding rate not < 20%.
Run length based approach for image splicing detection.[16]	Not lessened the influence of complex texture.	High detection accuracy with fewer features than other techniques.
Steganalysis of HMPD reversible data hiding scheme.[17]	----	Accurate upto 99.77%.
Ensemble Classifiers.[18]	Less accurate than G-SVM.	Better than SVM at a fraction of computational cost.
Richs Model for Steganalysis.[19]	Models require further investigation and optimization for better performance.	Automatizing steganalysis to facilitate fast development of accurate detectors for new steganographic schemes.
Steganalysis for histogram-shifting based reversible data hiding.[20]	Generalize reference templates can be introduced to improve performance.	Effective on stego-images detection and embedding locations at low bit rates.

iv. Conclusions

This paper outlined the brief introduction on steganaography and steganalysis. In the last decade many steganalytic techniques for digital media have been proposed in the literature. The various methods have been categorized as: Signature and Statistical Steganalysis. These are further classified as: Specific and Universal Steganalysis.

Here we focus on Statistical Steganalysis rather than Signature Steganalysis , because statistical steganalysis is more powerful than signature steganalysis as mathematical techniques are more sensitive than visual perception . After classification of steganalysis we have tried to make a note of various approaches used in the steganalytic methods that are applicable to digital images. Various techniques have been developed for detection of embedding data in images, some techniques are specific to particular steganography technique and some are applicable on any type of steganography technique. Techniques which are main focused in this paper are : Detection Of LSB Steganography based on the translation coefficients between difference image histogram; Stochastic Approach For Message Length Estimation in ±k Embedding Steganography; WAM ; Run length based technique for image splicing detection ; Steganalysis of HMPD reversible data hiding scheme ; SPM . Many types of classifiers are developed for distinguishing the cover image from stego-image. Popular classifiers are SVM , G-SVM , OC-SVM , ENSEMBLER etc. Steganalysis finds its use in computer forensics, cyber warfare, tracking the criminal activities over the internet and gathering evidence for investigations particularly in case of anti-social elements . These steganalysis techniques are developed for improving the security of steganographic tools by evaluating and identifying their weaknesses.

References

[1]. William Stallings, Cryptography and Network Security—Principles and Practices, fourth ed., Dorling Kindersley (Pearson Education, Pvt. Ltd.), India, 2004.

[2]. M.M. Amin, M. Salleh, S. Ibrahim, M.R. Kitmin, M.Z.I. Sham suddin, Information hiding using steganography, in: 4th Natl. Conf. on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003.

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

[4]. N.F. Johnson, S. Jajodia, Steganalysis: The investigation of hidden information, in: Proc. IEEE Information Technology Conference, Syracuse, NY, 1998 , pp.113-116.

[5]. Arooj Nissar, A.H. Mir, Classification of steganalysis techniques: A study, Digital Signal Processing, vol.20, Elsevier, 2010, pp 1758–1770.

[6]. Tariq Al Hawi, Mahmoud Al Qutayari, Hassan Barada, Steganalysis attacks on stego images using stego-signatures and statistical image properties, in: TENCON 2004, Region 10 Conference, vol. 2,2004, pp. 104 -107.

[7]. M. Goljan and R. Du, Reliable Detection of LSB Steganography in Grayscale and Color Images**,** *Proc. of the ACM Workshop on Multimedia and Security*, Ottawa, Canada, October 5(2001), pp. 27-30.

[8]. T.S. Holotyak and D. Soukal, Stochastic Approach to Secret Message Length Estimation in +-*k* Embedding Steganography, *Proc. SPIE Electronic Imaging* San Jose, CA, January 16-2-2005, pp. 673-684.

[9]. M. Goljan and T. Holotyak, *Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072, San Jose, CA, January 16-19-2006, pp. 1-13.

[10]. T. Holotyak, J. Fridrich, S. Voloshynovskiy, “Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics,” 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, LNCS vol. 3677, Springer-Verlag, Berlin, 2005,pp. 273–274.

[11]. Jing Dong , Tieniu Tan , “Blind Image Steganalysis Based On Run-Length Histogram Analysis”, IEEE image processing conference, 2008 ,pp.2064-2067.oct,2008.

[12]. Y. Shi, C. Chen, W. Chen, A Markov process based approach to effective attacking JPEG steganography, Lecture Notes in Computer Sciences 4437 (2007), pp.249–264.

[13]. Qingzhong Liu, Andrew H. Sung, Mengyu Qiao, Zhongxue Chen, Bernardete Ribeiro,“An improved approach to steganalysis of JPEG images”, Elsevier, Information Sciences 180 (2010),pp. 1643–1655.

[14]. T. Pevný and P. Bas, *IEEE Trans. on Info. Forensics and Security*, vol. 5(2),2010, pp. 215–224.

[15]. Hong Zhao, Hongxia Wang, Muhammad Khurram Khan, “Steganalysis for palette-based images using generalized difference image and color correlogram”,Elsevier,Signal Processing,vol.91 ,2011,pp. 2595–2605.

[16]. Zhongwei He, Wei Sun, Wei Lu, Hongtao Lu, “Digital image splicing detection based on approximate run length” ,Elsevier, Pattern Recognition Letters ,vol.32, 2011, pp.1591–1597.

[17]. Der-Chyuan Lou, Chen-Hao Hu, Chao-Lung Chou, Chung-Cheng Chiu “Steganalysis of HMPD reversible data hiding scheme”, Elsevier, Optics Communications ,vol.284 ,2011 , pp.5406–5414.

[18]. J. Kodovský and V. Holub, *IEEE Trans. on Info. Forensics and Security*, vol. 7(2), 2012, pp. 432-44.

[19]. J. Kodovský, *IEEE Trans. on Info. Forensics and Security*, vol. 7(3), 2012, pp. 868-882.

[20]. Der-Chyuan Lou, Chao-Lung Chou, Hao-Kuan Tso, Chung-Cheng Chiu “Active steganalysis for histogram-shifting based reversible data hiding”, Elsevier, Optics Communications 285 , 2012, pp.2510–2518.