ISSN: 2278 – 1323
*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*
*Volume 1, Issue 7, September 2012*

# AN EXTENSIVE REVIEW OF CURRENT TRENDS IN STEGANALYSIS

**Pratap Chandra Mandal**
**Asst. Prof. , Dept of Computer Application,**
**B.P.Poddar Institute of Management & Technology,**
**West Bengal, India**

***Abstract*: - Steganography refers to the art of secret communication while steganalysis is the art and science of detection of the presence of steganography. Both 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. Newer and more sophisticated steganographic techniques for embedding secret message will require more and more powerful steganalysis methods for detection. An extensive review of the current steganalysis methodologies has been presented in this paper.**

**Index Terms- Statistical, Signature, Steganalysis, Steganography,**

## 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 [1]. 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 .With the beginning of data hiding techniques the research on steganalysis started in the late 90's.Many advances are already done in the steganography but still its analysis part is not well developed [2]. Different researchers discussed various approaches .A steganalysis technique specific to an embedding method may give very good results when tested only on that embedding method, and might fail on all other steganographic algorithms. As reported by the USA TODAY AP by Jack Kelley that in 1998, Osama bin laden used the steganography technique to hide the information related to the bombing of two U.S embassies in East Africa. So, it becomes very necessary to work in the area of the detection of the hidden data. Past decade has been growing interest in researches on image steganography and steganalysis At present, more stress have been given to the Steganalysis than Steganography. So, attempt has been made to build up and employ few Steganalysis techniques. Existing techniques form a very small part of a very big system that calls for exciting and challenging research for the years to come [3]. In this paper an attempt has been made to make a note of the various approaches proposed for the steganalysis of images and classify them.

The rest of the paper is organized as follows: classification of steganalytic techniques is given in Section 2. Section 3 deals with steganographics tools followed by conclusion in section 4.

## II. STEGANALYSIS TECHNIQUES

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].The first specific statistical steganalytic tool Chi-Square Attack developed for detection of message bits from stego-images embedded by LSB steganographic tool .Specific statistical steganalysis can be further divided as follows:

**2.1.1. LSB embedding steganalysis**

LSB steganography has been one of the most important spatial steganographic techniques. 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 [5], RS analysis, sample pair analysis (SPA) analysis, weighted stego (WS) analysis, and structural steganalysis etc.

Many other steganalytic techniques [4] 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 [6]. 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 [7].

A technique in grayscale images is proposed by Zhang and Ping [8].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 [9] 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. [10] a proposed a steganalysis technique based on bit plane randomness tests. Two binary sequences are obtained by scanning the $7^{th}$ and $8^{th}$ 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 [11] , 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 [12], 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 [13] 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. [14], 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.** [15], 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.

### 2.1.2. LSB matching steganalysis

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 [16]. 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. [17] 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 [18] 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 [19], 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 [20]. 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.

### 2.1.3 Spread-spectrum steganalysis

Past several years spread spectrum (SS) data hiding has enjoyed a wide popularity in the data hiding community. Additionally SS hiding can be used for covert communication, i.e. steganography, which inevitably leads to others searching to detect the presence of this hidden communication.

In paper [21] Kenneth Sullivan et al. focused on the detection of hidden data. They have used Markov chain image model, statistical analysis of spread spectrum hiding under this model, and estimations of the detectability of various adaptations of SS hiding specifically they focused on detecting data hidden in grayscale images with spread spectrum hiding. They have used a statistical model of images and estimate the detectability of a few basic spread spectrum methods. They designed a tool for detecting hiding on various spread spectrum methods. They correctly detect the presences of hidden data in about 95% of images.

.

Chandramouli and Subbalakshmi [22] proposed two steganalysis schemes specific for spread spectrum steganography. First scheme is a simple estimate and subtract type algorithm which does not exploit higher order statistics. Assessment of cover image from stego image is done by standard regression techniques. The estimated value is subtracted from the stego image to get the estimate of the covert message. In second scheme an attempt has been made to blindly reverse the stego function using higher order statistics. Tests show that in comparison to simple estimation scheme exploiting higher order statistics improves performance of steganalysis.

The method given in [23], is applicable to images embedded with secret message using adaptive spread spectrum steganography. It is based on block based scatter difference detection. The cover image is first restored by a spatial filter. After that spread spectrum process is simulated on the test image several times and the scatter of low frequency coefficients in each DCT block is estimated. Same method is used over the estimated cover image with its own

scatter gained. The difference between two scatters is used to determine whether there is spread spectrum message in the test image or not. The experimental results are very promising.

Muhammad Khurram Khan et al. in paper [24] proposed a chaos and NDFT-based spread spectrum technique to conceal fingerprint-biometrics templates into audio signals. Fingerprint templates are encrypted by chaotic encryption, encoded by the BCH codes and modulated by chaotic parameter modulation.Experimental result and simulation results show that the proposed scheme is robust against common signal processing attacks.

**2.1.4. JPEG-Compression steganalysis**

JPEG compression is a normally used method for reducing the file size of an image, without reducing the visual qualities enough to become noticeable by the naked eye. Detection of information hiding in JPEG images is actively delivered in steganalysis community due to the fact that JPEG is a extensively used compression standard and several steganographic systems have been designed for secret communication in JPEG images. Due to the popularity of JPEG images on the Internet, efficient steganalysis techniques are developped to answer the threat of JPEG steganography.

In the paper [25] Jessica Fridrich et al. described a new steganolytic technique to detect modifications in digital images as long as the original image has been previously stored in the JPEG format. The steganalytic technique begins with extracting the JPEG quantization matrix by carefully inspecting the clusters of DCT coefficients in all 8×8 blocks. Then, each block is analyzed if its pixel values are truncated values of an opposite DCT transform of a set of coefficients quantized with the extracted quantization matrix. If the equivalent quantized DCT coefficients are found, the block is termed compatible, otherwise it is not.

In paper [26], a steganalysis method is discussed to effectively attack the advanced JPEG steganography schemes.This method used Markov empirical transition matrices to capture both intra-block and inter-block dependencies between block DCT coefficients in JPEG images. Features are extracted from observed transition matrices by a threshold technique.

Paper [27], presents a methods for detection of double -compression in JPEGs and for estimation of the primary quantization matrix, which is lost during recompression. The proposed techniques are essential for construction of accurate targeted and blind steganalysis methods for JPEG images, especially those based on calibration.

Qingzhong Liu et al. proposed a new approach based on feature mining on the discrete cosine transform (DCT) domain and machine learning for steganalysis of JPEG images in paper [28]. Neighboring joint density features on both intra-block and inter-block are extracted from the DCT coefficient array and the absolute array first; then a support vector machine is applied to the features for detection. Neural-fuzzy inference system is used to predict the hiding amount in JPEG steganograms. Experimental results show that, in detecting several JPEG-based steganographic systems, their method significantly outperforms the Markov-process based approach.

**2.1.5. Transform domain steganalysis**

Transform domain includes discrete Fourier transform, discrete cosine transform, discrete wavelet transform mainly. To combat the threat posed by steganography, steganalysis aims at the exposure of the stealthy communication.

Paper [29], presents neural network based steganalysis. Original as well as stego images are analyzed in DFT, DCT, DWT transform domains using neural network. Neural network computes the statistical features of images that are considerably impacted by data hiding. Results show that the method is hopeful.

S. Liu et al. [30] proposed another technique for the detection of wavelet domain information hiding techniques. The work is based on statistical analysis of the texture of the image. Neural network is used as a discriminator to distinguish between stego and clean images.

In paper [31], Jan Kodovský et al. constructs a new quantitative steganalyzers for steganographic techniques that hide data using LSB embedding in quantized DCT coefficients of a JPEG file. They have used two approaches: change-rate estimation using the maximum likelihood principle and a heuristic approach based on minimizing a penalty functional obtained from a combined analysis of the embedding operation and properties of natural images. These methods are used to Jsteg and its modified version called symmetric Jsteg.

Andreas Westfeld et al. [32] proposed a generic methodology to prepare higher order steganalytic techniques from spatial domain for application in the transformed domain. They presented the role of the proposed methods in terms of detection power and precision compared to prior art and determine how properties like image size and JPEG quality influence the ranking of the proposed attacks.

**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.

The first universal statistical steganalysis method is given by Memon and co-workers in [33]. They proposed a

steganalytic technique which exploit for detection of secret message using image quality metrics and multivariate regression analysis. They used analysis of variance technique to identify appropriate image quality metrics, which is fed to multivariate regression along with a training set of cover and stego-images.

Lie and Lin proposed a steganalytic method which uses the gradient energy and statistical variance as two features for detection of hidden messages in spatial or DCT domain [34].

In [35] Zou et al proposed a steganalytic method based on Markov model of threshold prediction error image.

Zhan and Zhang proposed a universal steganalytic method based on higher-order wavelet decomposition to detain statistical difference between the cover images and stego-images in paper [36].

Liu et al. proposed a universal steganalytic method based on wavelet packet transform that gives sub band coefficients, which in turn gives multi-order absolute characteristic function moments of histogram as features in paper [37].

In paper [38], Chen et al. proposed an image estimation method utilizing the alpha-trimmed mean for distinguishing cover images and stego-images. This method can estimate secret messages from images in spatial and JPEG compression domains.

In paper [39], Cho et al. projected a steganalytic technique which categorizes image blocks into multiple classes of steganalytic results of decomposed image blocks.

In order to attack especially domain steganographic algorithms, a novel universal steganalysis method is introduced in paper [40].Results of the proposed method is compared with the state-of-the-art steganalysers.

Chunhua Chen et al. [41] presented another new universal steganalysis method based on statistical moments.They have considered first & second order histogram. The moments of 2-D characteristic functions are also used for steganalysis. The experimental works have shown that the proposed technique surpasses the prior-arts of steganalysis methods.

Shaohui Liu, presented a new universal steganalysis method based on statistical models of the image's DCT coefficients in paper [42]. The experimental results shown that the proposed technique outperforms in general prior-arts of steganalysis techniques based on wavelet transform domain.

Paper [43] demonstrates that, when the secret message is embedded, the number of the different quantised discrete cosine transform (qDCT) coefficients and the symmetry of the qDCT coefficient histogram will be disturbed. Moreover, the intrinsic sign and magnitude dependencies will be disturbed too. Modern universal steganalysers can detect these disturbances.The authors have proposed two new steganalytic approaches. Through exploring the distortions these two alternative steganalysers can detect JPEG-CES effectively. By merging the features of these two steganalysers, a more reliable classifier can also be obtained.

## III. STEGANALYTIC TOOLS

There are various steganalytic tools available in market like: PhotoTitle, Benchmark, StirMark and 2Mosaic etc [44]. 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.

## IV. CONCLUSION

Critical review of the current Steganalysis algorithms has been presented in this paper. I can expect that this paper will give 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. The battle between steganography and steganalysis is never ending. Newer and more sophisticated steganographic techniques for embedding secret message will require more powerful steganalysis methods for detection.

The various methods have been categorized. From the information of the methods reported in this paper we have understood that statistical steganalysis techniques, in any domain, are more robust and give promising results than signature steganalysis. Such steganalytic techniques specific to a steganographic embedding method yield accurate decisions when tested only on that method and may fail if any other steganographic technique is used.

Since a steganalyst will not be able to know what steganographic technique is used, using a specific statistical steganalysis method may not be reasonable. Instead a universal statistical steganalysis technique may work provided it successfully detects any steganographic embedding algorithm. Hence there is still an utmost need of a steganalysis method which could detect any type of steganographic embedding algorithm.

The research to device strong steganalysis technique is a continuous process and still going on.

**REFERENCES**

[1]. Natarajan Meghanathan and Lopamudra Nayak,"STEGANALYSIS ALGORITHMS FOR DETECTING THE HIDDEN INFORMATION IN IMAGE, AUDIO AND VIDEO COVER MEDIA, "international journal of Network Security & Its application (IJNSA) ,Vol.2 No.1 ,Jan-2010,pp.43-55

[2] SWAGOTA BERA , MONISHA SHARMA, "STEGANALYSIS OF REAL TIME IMAGE BY STATISTICAL ATTACKS," International Journal of Engineering Science and Technology Vol. 2(9), 2010, pp.4396-4405

[3] Yambem Jina Chanu, Kh. Manglem Singh ,Themrichon Tuithung, " Image Steganography and Steganalysis: A Survey," International Journal of Computer Applications (0975 – 8887) Volume 52– No.2, August 2012 ,pp.1-11

[4] 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

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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

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

[13] 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

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

[15] 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

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

[17] 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.

[18] 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

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

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

[21] Kenneth Sullivan, Upamanyu Madhow, Shivkumar Chandrasekaran, and B.S. Manjunath," Steganalysis of Spread Spectrum Data Hiding Exploiting Cover Memory" http://vision.ece.ucsb.edu.

[22] R. Chandramouli, K.P. Subbalakshmi, "Active steganalysis of spread spectrum image steganography", IEEE Int. Symp. on Circuits and Systems, Bangkok, Thailand, vol. 3, May 2003, pp. 830–833.

[23] Ji Rongrong, Hongxun Yao, Shaohui Liu, Liang Wang, Jianchao Sun, "A new steganalysis method or adapting spread spectrum steganography," in: Proc. IEEE Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, 2006.

[24] Muhammad Khurram Khan , Ling Xie, Jiashu Zhang," Chaos and NDFT-based spread spectrum concealing of fingerprint-biometric data into audio signals, " Digital Signal Processing 20 (2010)pp. 179–190

[25] Jessica Fridrich, Miroslav Goljan, Rui Du " Steganalysis Based on JPEG Compatibility"

[26] Fu Dongdong, Yun Q. Shi, Dekun Zuo, Guorong Xuan,"JPEG steganalysis using empirical transition matrix in block DCT domain, " in: IEEE 8th Workshop on Multimedia Signal Processing, October 2006, pp. 310–313

[27] Tom´aˇs Pevn´ya, Jessica Fridrich," Estimation of Primary Quantization Matrix for Steganalysis of Double-Compressed JPEG Images,", Proc. of SPIE-IS & T Electronic Imaging, SPIE Vol. 6819, 681911, © 2008

[28] Qingzhong Liu,Andrew H. Sung , Mengyu Qiao," Neighboring Joint Density-Based JPEG Steganalysis,"NewMexico Tech, ACM Transactions on Intelligent Systems and Technology, Vol. 2, No. 2, Feb. 2011.,pp.16.1-16.16

[29] Shaohui Liu, Yao Hongnun, Wen Goa, "Neural network based steganalysis in still images,{" Proc. Int. Conf. on Multimedia and Expo, ICME2003, vol. 2, July 2003, pp. 509–512.

[30] Shaohui Liu, Hongxun Yao, Wen Goa, "Steganalysis based on wavelet texture analysis and neural network,"Proc. of WCICA 2004, HangZhou, China, 2004.

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

[32] Andreas Westfeld, K. Solanki, K. Sullivan, and U. Madhow," Generic Adoption of Spatial Steganalysis to Transformed Domain," Springer-Verlag Berlin eidelberg 2008 ,, LNCS 5284, pp. 161–177.

[33] I. Avcibas , N. Memon and B. Sankur," Steganalysis using image quality metrics," Security and Multimedia Contents, SPIE, 2001.

[34] W-N. Lie and G-S. Lin," A feature based classification for blind image steganalysis," IEEE Transaction Multimedia, vol. 7, no. 6, pp. 1007-1020, December 2005.

[35] D. Zou, Y. Q. Shi, W. Su and G. Xuan," Steganalysis based on Markov model of threshold prediction-error image," IEEE ICME, 2006.

[36] S-H. Zhan and H-B. Zhang," Blind steganalysis using wavelet statistics and ANOVA," IEEE Conference on Machine Learning and Cybernetics, vol. 5, pp. 2515-2519, 19-22 August, 2007.

[37] X. Luo, F. Liu, J. Chen and Y. Zhang," Image universal analysis based on wavelet packet transform," 10th IEEE Workshop on Multimedia Signal Processing, pp. 780-784, 2008.

[38] M-C. Chen, S.S. Agaian, C.I.P. Chen and B.M. Rodriguez, "Alpha -trimmed image estimation for JPEG steganography," Proc. of IEEE International Conference Systems, Man and Cybernetics, pp. 4581-4585, 2009.

[39] S. Cho, B-H. Cha, J. Wang and C-C. J. Kuo,"Block based image steganalysis: Algorithm and performance evaluation," Proc. on IEEE ISCAS, pp. 1679-1682, 2010.

[40] Gokhan Gu1 , Fatih Kurugoll , "A NOVEL UNIVERSAL STEGANALYSER DESIGN:LOGSV"

[41] Chunhua Chen, Yun Q. Shi, Wen Chen , Guorong Xuan, " STATISTICAL MOMENTS BASED UNIVERSAL STEGANALYSIS USING JPEG 2-D ARRAY AND 2-D CHARACTERISTIC FUNCTION "

[42] Shaohui Liu, Lin Ma, Hongxun Yao, Debin Zhao ,"Universal Steganalysis Based on Statistical Models Using Reorganization of Blockbased DCT Coefficients," Fifth International Conference on Information Assurance and Security, 2009.

[43] F. Huang W. Luo J. Huang, ET, " Steganalysis of JPEG steganography with complementary embedding strategy," Inf. Secur., 2011, The Institution of Engineering and Technology , Vol. 5, Iss. 1, pp. 10–18

[44] VIPUL SINGHAL, DHANANJAY YADAV, DEVESH KUMAR BANDIL," STEGANOGRAPHY AND STEGANALYSIS: A REVIEW," INTERNATIONAL JOURNAL OF ELECTRONICS AND COMPUTER SCIENCE ENGINEERING, VOLUME1,NUMBER 2,PP.399-404

**Mr. Pratap Chandra Mandal** received the MCA degree from North Bengal University and M.E.(CSE) from West Brengal University of Technology .He is a Assistant Professor in B.P.Poddar Institute of Management & Technology, West Bengal ,India . He has published 2 papers in international Journal. His research interests include Cryptography, Steganography and Image Processing.