Defend against Adaptive Stenographic Attack using Mx-Quadrtree Neighbor Finding Mechanism

Dr.T.Pandikumar[1], Habtewold Desta[2]

[1]PhD Department of Computer & Information Technology, Defence University College of Engineering, Debre Zeyit, Ethiopia
[2]M.Tech Department of Computer & Information Technology, Defence University College of Engineering, Debre Zeyit, Ethiopia

---

Abstract - *The major threat in cybercrime for digital forensic examiner is to identify, analyze and interpret the concealed information inside digital medium such as image, audio and video. The most interesting thing in this title and that motivates me to study in this area is the way how to extract a message from any kind of stago image. This kind of extraction and translation helps the defense to take action and to identify what is going inside and who is the one doing this. In the world of information security, Trapping of Illegal secret communication plays an imperative role. Especially, defending against such type of attacks plays important role in the area of defense. Steg analysis is the countermeasure against steganography. Steg analysis deals with the extraction of hidden data from the cover media. The cover media could be an image or an audio or a video file. Human Visual System (HVS) may not clearly identify the images with hidden information. Universal Steg analysis is the method of attacking the Stego images regardless of the method used for embedding secret information into the cover media. Universal Steg analysis is a combination of two methods; they are feature extraction and classification. Most research papers that focus in Steg analysis uses extraction methods and some uses signature steg analysis and statistical steg analysis. The research paper we found called* ***Universal Steg analysis*** *uses extraction and classification. And it uses Adaptive steganography as it is a perceptual masking technique which is based on color contrast of the image. This type of steganography does not modify the image quality, which has higher rate of embedding capacity and un-perceivability. This features of the paper attracted us to review and make it our title.*

Key Words*:* Steganogrpahy;MX-Quadtre, Adaptive Steg Analysis

1. INTRODUCTION

Steganalysis is a method of extracting the unrevealed messages from the cover media. Adaptive steganalysis attempts to extract the concealed messages which are embedded based on the color nature of the cover media. Universal steganalysis also called as blind steganalysis, which attempts to attack the stego images without any prior knowledge about the stenographic algorithm used. Universal steganalysis is a combination of feature extraction and feature classification. From the data set of images; a group of statistics is obtained based on the features of the image. These extracted features are used to train a classifier to identify the cover and stego image. The neighboring joint features are extracted on intra block and inter block from the Discrete Cosine Transform Coefficient arrays. Quad tree mechanism is an optimized technique, which reduces the number of recursive calls.

1.1 Statement of the Problem

In the world of information security, Trapping of Illegal secret communication plays an imperative role. Especially, defending against such type of attacks plays important role in the area of defense. Steg analysis is the countermeasure against steganography.

1.2 Objectives of the Research Papers

The objective of this paper is to extract a stego image for the purpose of defense and identifying the data or information transferred between the targets. That means the information transferred maybe secrete and not to be given to outsiders or unauthorized group that may cause a damage.

1.3 Significance of these research works

This paper has high significance for the defense work. In that it helps to now the information inside the stego image without knowledge of the algorithm used. And can give full information to the needy.

1.4 Literatures Referred

1.4.1 Review of Various Steganalysis Techniques
1.4.2 Steganalysis using color model conversion
1.4.3 A Review on Steganalysis Techniques: From Image Format Point of View
1.4.4 Steganlysis algorithms for detecting the hidden information in image audio and video cover media
1.4.5 New Steganalysis Method using Glcm and Neural Network

2. STEGANALYSIS SYSTEM

2.1. Steganalysis

In recent years, digital watermarking has emerged as an increasingly active research area. Information can be hidden into images, videos, and audios imperceptibly to human beings. It provides vast opportunities for covert communications. Consequently, methods to detect covert communications are called for. This task is especially urgent for law enforcement to deter the distribution of exceptional images/videos hidden inside normal images/videos, and for intelligence agencies to intercept communications of enemies.

Steganalysis is the art and science to detect whether a given medium has hidden message in it. On the other hand, steganalysis can serve as an effective way to judge the security performance of stenographic techniques. In other words, a good stenographic method should be imperceptible not only to human vision systems, but also to computer analysis.

The huge diversity of natural images and the wide variation of data embedding algorithms make steganalysis a tough mission. However, an original cover medium and its stego-version (with hidden message inside) always differ from each other in some aspects since the cover medium is modified during the data embedding. A method designed to blindly detect stego-images is referred to as a universal steganalysis method, meaning it does now know which specific data hiding method is actually used and it does not have the original image in detection. From this point of view, the universal steganalysis methods have more real value for deterring covert communications.

2.2 Universal Steganalysis

Current steganalysis for images is not universal, which is usually special for one kind of steganography and not practical for others. Meanwhile the correct detection rate of these detecting methods is not high. After analyzing current steganalysis methods, a new steganalysis method for detection of steganography in image's frequency domain is proposed. The detecting method is universal and is not restrained to some special steganography method. Based on the spectrum analysis of difference histogram of frequency coefficients, the detection is achieved according to evident spectrum difference between non-steg-images and steg-images

Universal steganalysis techniques work by designing a classifier based on a training set of cover objects and stego-objects obtained from a variety of different embedding algorithms. Classification is done based on some inherent “features” of typical natural images which can get violated when an image undergoes some embedding process. Hence, designing a feature classification based universal steganalysis technique consists of tackling two independent problems.

The first is to find and calculate features which are able to capture statistical changes introduced in the image after the embedding process.

The second is coming up with a strong classification algorithm which is able to maximize the distinction captured by the features and achieve high classification accuracy. There have been a number of Universal steganalysis techniques proposed in the literature, these techniques differ in the features sets they propose for capturing the natural image statistics.

Detection accuracy can be interpreted as the ability of the features to detect the presence of a hidden message with minimum error on average.

These are three techniques, which would highlight different approaches in obtaining the features which will be used in steganalysis.

2.2.1 Wavelet Based

A different approach is taken for feature extraction from images. Quadratic mirror filters (QMF) are used to decompose the image into wavelet domain, after which higher order statistics such as mean, variance, skewness, and kurtosis are calculated for each sub-band. Additionally the same statistics are calculated for the error obtained from an optimal linear predictor of coefficient magnitudes of each sub-band, as the second part of the feature set

2.2.2 Feature Based

Feature based is used to estimate statistics of the original image. Estimation is simply done by decompressing the JPEG image, and then cropping its spatial representation by 4 pixels. After words the image is re-compressed to JPEG using the original quantization table. The obtained image will have statistical properties very much similar to the original image, before any introduced distortions. The difference between statistics obtained from the given JPEG image, and its original estimated version are obtained through a set of functions which operate on both spatial and DCT domain

2.2.3 Classifier

In all of the above methods, the calculated features are used to train a classifier, which in turn is used to classify cover and stego images. A number of different classifiers could be employed for this purpose. Two of the more widely techniques used by researches for universal steganalysis are fisher linear discriminate (FLD), and support vector machines (SVM).

Support vector machines are more powerful, but on the down side, require more computational power, especially if a non-linear kernel is employed.

2.2.4 Confusion Test

A good classification based technique needs to have high detection rate, at the same time a small false alarm rate.

Some of the stenographic embedding techniques re-compress the JPEG image, before embedding the message in them. Thus false alarm could be caused by the classifier misclassifying images because of the re-compression artifacts.

The two cases of re-compression:

1. Re-compressing image with the quality factor estimated from the original image. This type of re-compression is seen with Outguess and F5 embedding technique which we will discuss later.

2. Re-compressing images with a quality factor smaller than the original quality factor. Such re-compression is seen with the PQ technique.

2.3 Embeddeing Techniques

As mentioned earlier, the concentration of the work is only on techniques which operate on JPEG images. Most of the work in this category has been concentrated on making use of redundancies in the DCT (discrete cosine transform) domain, which is used in JPEG compression Although changing the DCT coefficients will cause unnoticeable visual artifices, they do cause detectable statistical changes. In order to minimize statistical artifacts left after the embedding process, we can use different methods for altering the DCT coefficients, namely Outguess and F5, but, first decide on how to set the message size used in the embedding process. There have been 3 approaches in setting the message size when creating stego datasets:

1. Set message size relative to the number of non-zero DCT coefficients. Using this approach with embedding techniques, which only utilize non-zero DCT coefficients, guarantees a set number of modified coefficients in the data set.
2. Set constant message size. In such approach message sizes are fixed irrelative of the image size.
3. Set message size relative to image size. Again here, we could have two images of the same size, but with different number of changeable coefficients.

2.3.1 Outguess

Outguess, is an embedding algorithm which embeds messages in the DCT domain. Outguess goes about the embedding process in two separate steps.

First it identifies the redundant DCT coefficients which have minimal effect on the cover image, and then depending on the information obtained in the first step, chooses bits in which it would embed the message. One of its goals was to overcome steganalysis attacks which look at changes in the DCT histograms after embedding.

The code for Outguess is publicly available. The code is implemented quite efficiently in C. As part of the embedding process, the Outguess program, first re-compresses the image, to quality factor defined by the user, and then uses the obtained DCT coefficient to embed the message. Here in order to minimize the re-compression artifact there should be a way to pass in the estimated quality factor of the image to the Outguess program.

2.3.2 F5

F5 code is also publicly available; the code is written in JAVA. Similar to Outguess, the available implementation of F5, first re-compresses the image, with a quality factor inputted by the user, after which the DCT coefficient are used for embedding the message. The quality factor estimated for each image is used as an input to the F5 code, when embedding a message. Messages of length and BPNZ-DCT should be used to create the stego data set. The re-compressed images are obtained by re-compressing them using their estimated quality factor.

3. DEFERENT STEG ANALYSIS METHODS

3.1 Colour Model Conversion Mechanism

This mechanism focuses on universal image steg analysis method which uses RGB to HSI color model conversion. It is based on statistical analysis of pixel pairs using their RGB components to detect the presence of hidden messages in LSB steganography.

Here the Cover image and Stego-Image is differentiated by **threshold value**. This threshold value **depends on the correlation between pixel pairs** in terms of color components. Apart from threshold value **unique color component also plays** a major role in **finding out** the **Stego-Images**. The LSB Steganalysis method through Color Pair Value Variable threshold which is derived from Color Density of the image [2].

In this method, a technique called Color Model conversion was used for discriminating the clean image and stego image (generated from LSB technique). The method was tested on Stego-image produced by Stego-Image Generator (SIG) tool implemented by Math lab 7[2].

3.2 Independence With Image Format Mechanism

This method is **based on statistical characteristic** of **multi-domain features extraction**, mainly aimed at detecting hidden information in images with multiple common formats. Features are firstly extracted in contour let domain and extended to spatial domain afterwards, by **calculating correlation between DCT (discrete cosine transform) coefficients** using joint probability density and calculating distribution of coefficients in image using co-occurrence matrix.

Consistency of contour let domain features is first taken into account when extracting features from images in all

formats. As embedding methods at present are mainly based on DCT domain, a co-occurrence matrix and correlation of DCT coefficients were used to describe changes of statistical features when embedding secret messages, combined with characteristics of spatial domain extracted from all carrier images. A support vector machine is used as a classifier in order to achieve the correct classification [5].

3.3 Texture And Noise Feature Mechanism

Firstly, this method uses **local linear transform to extract image texture** features. Secondly**, it extracts image noise features from three areas: wavelet analysis, image de-noising and neighbor prediction**. Thirdly, it calibrates all income characteristics to make them reflect the changes of embedded information better. Finally, it exploits support vector machine for feature classification to whether the image contains hidden information.

Here blind detection method is **based on texture and noise features**, using images of additive noise model by the way of 'pretreatment and feature extraction and classification'. This method of extracting image features from local linear transform domain, wavelet analysis, image demising and neighborhood prediction enhance the sensibility of features. And, it makes detection rate a certain extent enhanced by supporting vector machines. Experimental results show that this method has good detection effect on LSB, Cox's SS, F5 and JPhide, very ideal especially on JPhide. True positive rate and true negative rate will be up to 90% when the information embedding strength is slightly larger [6].

3.4 Quad Tree Mechanism

In this mechanism **there are two types of Image segmentation** based approximation they are. Region based and Curvilinear based image segmentation.

1) Region based Image segmentation deals about the **interior part of the region** by constructing a tree structure.

2) Curvilinear based image segmentation explains about **boundaries of the region**. A quad tree is a tree data structure in which nodes are leaves of 4 children. The root is the image taken for consideration and the children of the node represents 4 quadrants [1].

Leaves of the tree identify the uniform region of the image. For binary images zero '0' represents black and one '1' represents white. For color images it is shown in Fig. 1.

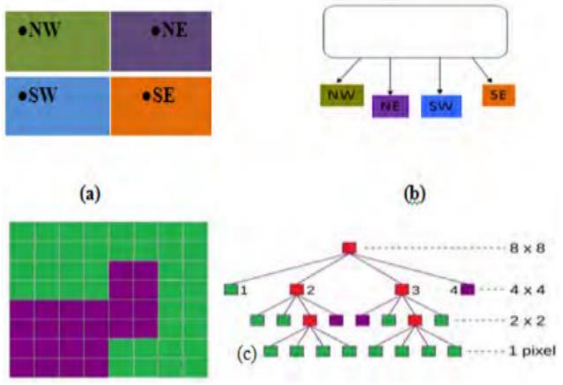

Fig 1: Quad tree mechanisms

4. METHODOLOGY

Simple block diagram for steg analysis process from stego image to message extraction

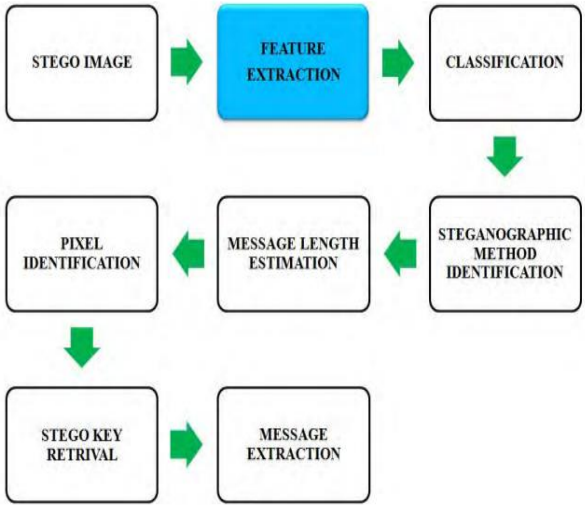

Fig 2: Block diagram for adaptive steg analysis

4.1 Stego Image Extraction

Here is how MX Quad tree neighbor finding mechanism extracts stego image. Image gets split into blocks of 2 X 2then applies MX Quad tree mechanism recursively to get the non-overlapping Quadrant squares based on color, select a pixel in the quadrant then check its value with the neighbor pixel value which should be same. If not, verify the pixel value with next non overlapping block of same color then we could find the Least Significant Bit (LSB) embedded ratio of adaptive steganography in number of bits per pixel (bpp).

MX Quad tree neighbor finding mechanism is highly flexible and easy for finding and differentiating the payload location of message. The remaining thing to be

done is feature extraction of hidden message. Matrix Quad tree mechanism is shown in Fig.3

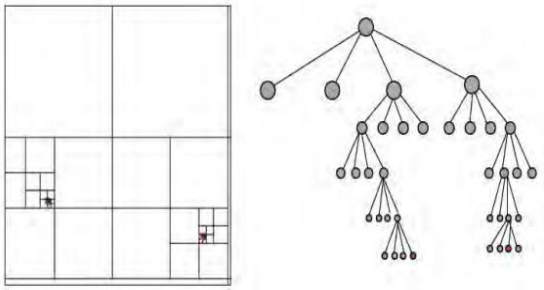

Fig 3: MatriX Quadtree Representation.

4.2 Feature Extarction

Here is how feature extraction done on stego image extracted. The feature extraction method considers the stego image which is divided it into blocks of (2^k X 2^k). Then Padding of image is done so that the image can be represented in a standard size format. So that XLB=0, XUB=2^k, YLB=0, YUB=2^k initialized. Then 'N' is considered as the original stego image and then finding the XLB, XUB, YLB, YUB of four Quadrants (North West, South West, North East and South East) of the image would be, as given in Table 1,

QUADRANT	XLB	XUB	YLB	YUB
NW	N.XLB	N.XLB+(ω/2)	N.YLB+(ω/2)	N.YLB+ω
SW	N.XLB	N.XLB+(ω/2)	N.YLB	N.YLB+(ω/2)
NE	N.XLB+(ω/2)	N.XLB+ω	N.YLB+(ω/2)	N.YLB+ω
SE	N.XLB+(ω/2)	N.XLB+ω	N.YLB	N.YLB+(ω/2)

Table 1: Quadrant calculations of 'N'

Where w is the width of the block represented by 'N'. Repeat the initialization process for getting the individual pixel value. Finally identify the adaptive region blocks by considering maximum sized block to minimum sized blocks so that the adaptive region could be found.

5. IMPLEMENTATION

Classification of images with and without embedded message is done by using Support Vector Machine Classifier (SVM). The SVM classifier trains the images based on inter pixel dependencies and classify it as stego or cover images.

The MX quad tree structure of the stego images based on their Color models. Fig.4 Represents the stego images which gets padded into a standard size, and fig.5 Represent MX Quadtree algorithm is applied on padded images to identify the color block i.e. adaptive regions of the image where the hidden messages could be, which is represented in fig.6.Payload location identification is represented in Fig.7

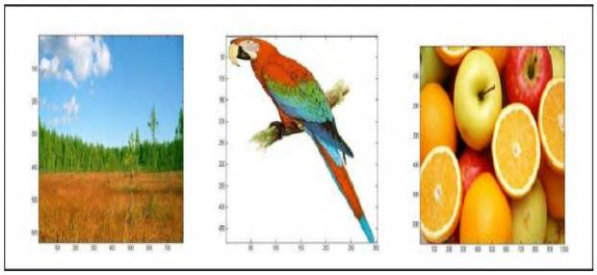

Fig 4: Stego images

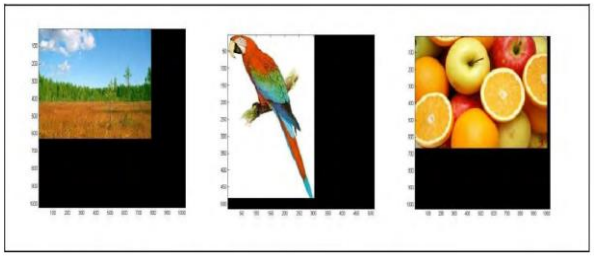

Fig 5: Padded Stego images

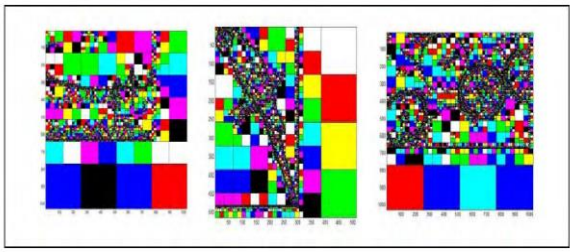

Fig 6: MX Quad tree representation of Padded Stego images

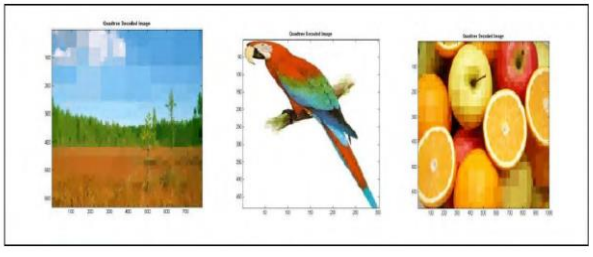

Fig 7: MX Quad tree decoded image which represents the payload location in form of blocks.

6. ANALYSIS

The performance of MX Quad tree neighbor finding is measured on color adaptability during embedding the messages, which are formed as quadrants on adaptive

steganalysis. The accuracy is estimated by considering bits per pixel (bpp) on the stego images. The quadrants of adaptable regions are grouped on which analysis can be done for identifying the stego messages. True positive rate (TPR) is used to identify the detection rate of stego images from the set of stego images and cover images. If TPR value is very close to 1 then it means that the detection accuracy and sensitivity is higher and the TPR is calculated by using the formula,

$$TPR = \frac{TP}{(TP+FN)} \quad (1)$$

Where, TPR is True Positive Rate and FN is False Negative True Positive, False Positive, False Negative and True Negative are explained for identifying the stego images using classifier output. Pearson correlations, mean square error (MSE), Structural SIMilarity Index (SSIM), false positive and false negative, were proposed to produce the performance of comparison between original and watermarked images.

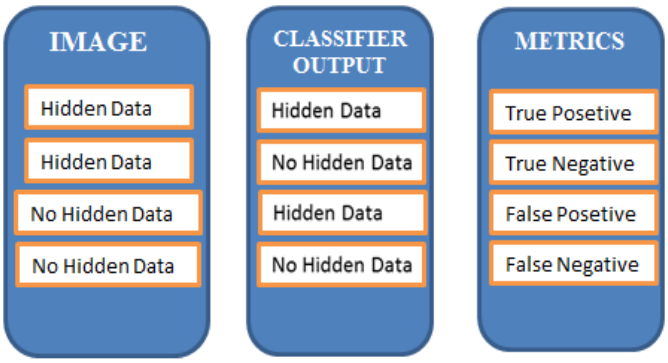

Table 2: Metrics for classification representation

Feature Extraction methods such as Wavelet Based, Empirical transition Matrix, Feature Based and MX Quad tree method are compared with three different steganalysis method with different embedding ratio of about 0.05 bpp i.e. For every 100 pixels 5 pixels are used for embedding and 0.1bpp i.e. For every 10 pixels 1 pixel is used for embedding. Dataset of about 900 images is used for analysis in which 500 images are stego images and 400 images are cover images.

The analysis table is as shown in Table 3 and its corresponding graphical representation is shown in Fig.8,

Feature Extraction		Wavelet Based			Empirical Transition Matrix			Feature Based			MX Quad tree		
Steg analysis Methods	Embedding ratio	TP	FN	TPR	TP	FN	TPR	TP	FN	TPR	TP	FN	TPR
Outguess	0.05	433	82	0.84	436	84	0.84	386	152	0.72	872	65	0.93
Outguess	0.1	450	120	0.79	400	150	0.73	432	89	0.83	923	52	0.95
F5	0.05	487	53	0.9	462	198	0.7	523	114	0.82	500	33	0.94
F5	0.1	365	72	0.84	350	300	0.54	586	147	0.8	432	45	0.91
MB1	0.05	536	95	0.85	493	152	0.76	682	152	0.82	300	52	0.85
MB1	0.1	458	83	0.85	384	83	0.82	735	69	0.91	275	35	0.89

Table 3: True positive Rate analyses for the dataset with different Steganalysis methods

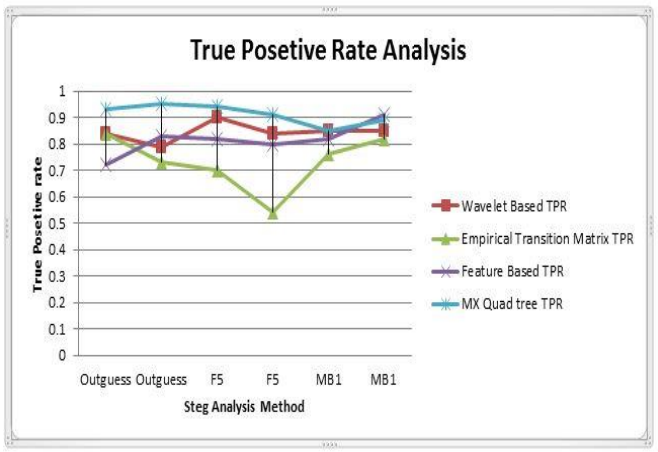

Fig 8: Graphical Representation of True Positive Rate Analyses.

MX-Quad tree based image segmentation for blind steg analysis is compared with quad tree, wavelet based, empirical transition matrix, and feature based image segmentation for steg analysis. It accounts for tree structure based image segmentation and information retrieval. Moreover, MX- Quad tree based image segmentation helps in accurately finding the adaptive region in the form of blocks so that the payload locations can be easily identified compared to the wavelet based, empirical transition matrix, and feature based image segmentation. Payload locations are identified from the blocks of quad tree using neighbor finding mechanism. In which, each pixel value is compared for recognizing the payload locations of adaptive region for better accuracy. It is indeed to consider the performance of the existing methods for classification of stego images and cover images, in MX quad tree neighbor finding mechanism binary classifier named Support Vector Machine (SVM) is used for better performance. **The metrics used** to measure the performance is True positive Rate (TPR) which lies between **0.85 to 0.95**.Thus the proposed method should be considered as an alternative method for point region based image segmentation in blind image steg analysis along with neighbor finding mechanism and Support Vector Machine (SVM) Classification.

7. CONCLUSION AND FUTURE RESEARCH WORK

The Table and Graph implies that MX Quadtree Feature Extraction method works better when compared to rest of steganalysis methods used for extraction with different feature extraction techniques and different embedding rate. The MX Quadtree method determines the payload location of jpeg images with True Positive Rate of about 95% when the bit per pixel is 0.10 for outguesses steg analysis method. MX Quadtree method works well in identifying payload location for an adaptive steganography. As mentioned above, analysis shows that MX Quadtree mechanism is an effective method which is used to detect the payload locations. Extraction of Embedded message could be the future work after finding the payload location and Identification.

REFERENCES

[1]. B.Yamini et al and Dr.R.Sabitha" UNIVERSAL STEGANALYSIS: DEFEND AGAINST ADAPTIVE STEGANOGRAPHIC ATTACK USING MX-QUADTREE NEIGHBOR FINDING MECHANISM" Indian Journal of Computer Science and Engineering (IJCSE) Vol. 6 No.6 Dec 2015-Jan 2016.

[2]. P.Thiyagarajan, G.Aghila and V. Prasanna Venkatesan "STEGANALYSIS USING COLOUR MODEL CONVERSION" An International Journal (SIPIJ) Vol.2, No.4, December 2011

[3]. 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, January 2010.

[4]. Sedighe Ghanbari, Manije Keshtegary and Najme ghanbari "New Steganalysis Method using Glcm and Neural Network" International Journal of Computer Applications (0975 – 8887) Volume 42– No.07, March 2012.

[5]. QiuyuZhang*, QichangShang,Ruihong Dong, YanYan, HangzhouZuo "A Method of Universal Steganalysis Using Independence with Image Format" 3rd International Conference on Multimedia Technology （ICMT 2013

[6]. Zhang Qiuyu, Hong Min, Li Liting, Huang Yibo" Blind Image Steganalysis Based on Texture and Noise Features" International Journal of Digital Content Technology and its Applications(JDCTA) Volume6,Number2,February 2012

[7]. http://ieeexplore.ieee.org

BIOGRAPHIES

Mr Habtewold Desta is Assistant Lecturer in School of Computing And Informatics at Mizan-Tepi University and Student of Networking and information security at Defense University College of Engineering.