**Abstract**

Hiding information within digital media will alter some of the media properties that may introduce few degradation or unusual characteristics. These characteristics may act as signatures that broadcast the existence of the embedded message, thus defeating the purpose of steganography. But such distortions cannot be detected easily by the human perceptible system. Without knowing which tool is used, detecting the hidden information may become quite complex.

Essentially there are two approaches to the steganalysis: one is to come up with steganalysis techniques that are specific to a particular steganographic technique. The other is developing universal techniques which are independent of the steganographic algorithm being used to hide the information. We are going to use universal steganalysis technique.

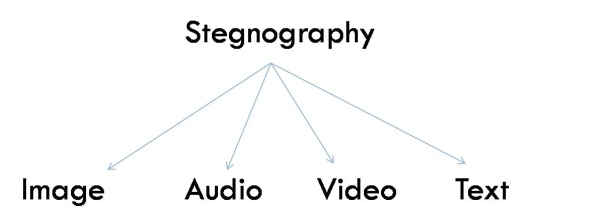
**Chapter 1**

**Introduction**

* 1. **Steganography[1]**

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning writing” defining it as “covered writing”.

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially fulfill this requirement. Figure 1 shows the four main categories of file formats that can be used for steganography.



***Figure 1 Categories Of Steganography***

Text steganography basically hide a secret message in **every *nth letter*** *of every word of a text message. For Example,*

*Since Everyone Can Read, Encoding Text*

*In Neutral Sentences Is Doubtfully Effective*

**Message**: ***Secret inside***

Not used very often since text files have a very small amount of redundant data.

**Digital images are most popular carrier for steganography**. As digital images are most popular especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image.

To hide information in audio files similar techniques are used as for image files. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images.

* 1. **Popular image steganography methods[1]**

Image steganography methods can be categorized into spatial and transform domain. spatial domain techniques embed messages in the intensity of the pixels directly, while for transform domain also known as frequency domain, images are first transformed and then the message is embedded in the image.

* + 1. **Spatial domain Steganography**

**LSB Insertion Technique**

Replaces least significant bits with the message to be encoded Most popular technique when dealing with images Simple, but susceptible to lossy compression and image manipulation. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

* + 1. **Transform domain Steganography**

In transform domain DCT based approach is most popular. In that Jsteg, Outguess and F5 are largely used for steganography now a days. This all are JPEG steganography. All this JPEG steganographic method embed the message in quantization table before the Huffman coding.

The JSteg algorithm was among the first algorithms to use JPEG images. In Jsteg first obtain DCT of image.Apply Quantization on DCT image. After quantization, Jsteg replaces (over writes) the least significant bits (LSB) of the frequency coefficient by the secret message. Resistant against the visual attacks and good capacity with 12.8 % of the steganogram's size, but the secret message is easily detected by statistical attacks.

Outguess Proposed by Provos, embedding algorithm which embeds message in DCT domain. Embedding process in two steps: It identifies the redundant DCT coefficients which have minimal effect on the cover image. In second step 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. So, proposed a solution in which some of the DCT coefficients are left unchanged in the embedding process, afterwards, these remaining coefficients are adjusted in order preserve the original histogram of DCT coefficients.

F5 embeds the information in DCT coefficient. It uses permutative straddling and matrix encoding. The straddling mechanism used with F5 shuffles all coefficients using a permutation first. Then, F5 embeds into the permuted sequence. The shrinkage does not change the number of coefficients only their values). The permutation depends on a key derived from a password. Matrix encoding decreases necessary number of changes. It follows specific atrix encoding algorithm.

**1.3 Steganalysis**

The general motivation for steganalysis is to remove the veil of secrecy desired by the hider. Typical uses for steganography are for espionage, industrial or military. A steganalyst may be a company scanning out going e-mails to prevent the leaking of proprietary information or an intelligence gatherer hoping to detect communication between adversaries.

**1.3.1 Introduction of image steganalysis**

Steganalysis is the art of detecting the presence of hidden messages. Hiding information within image requires alteration of the image properties that may introduce some form of degradation or create unusual characteristics. These characteristics may act as signature that broadcast the existence of embedded message, thus breaking the steganography system.

Attacks and analysis on hidden information may take several forms: Detecting, Extracting, Disabling, Destroying or Modifying the hidden information. Detecting messages or their transmission and disabling embedded information are varying depending upon the methods used to embed the information into cover image. Generally speaking making decisions about the presence or absence of embedded messages in cover image is essential to image steganalysis. Steganalysis algorithm is required to possess other properties such as low complexity and low classification risk. A low complexity algorithm makes the system capable of inspecting objects at a higher throughput rate and algorithm at of low classification risk generally makes tradeoffs between cost resulting from missing errors (i.e. false negative) and from false alarms (i.e. false positive).

**1.3.2 Importance of Image steganalysis**

Image steganalysis is the science of analyzing images in order to discover methods of discovering and detecting hidden messages and data within the images. Statistical digital signal processing is often used in order to detect data within images.

It is important to detect hidden messages within the images. On the steganography side this is important in order to find methods in order to improve algorithm implementing steganography. By exposing the flaws to the algorithm, the user can further improve the algorithm in order to make it more difficult to break whether or not data is hidden in the images.

Steganalysis is also especially important in the security aspect, namely monitoring a user’s communication with the outside world. In the age of internet images are sent via e-mail or by posting on websites. Detecting whether or not data is hidden in the images will allow the monitor to further analyze the suspicious images in order to find what the hidden message is.

**1.4 Approaches to Image Steganalysis**

There are two categories into which steganalysis method can be divided. One is *Specific steganalysis* and other is *universal steganalysis* that are effective over wide varity of steganographic techniques.

Specific steganalysis attack concentrate on image features which are directly modified by the embedding algorithm. Specific steganalysis fully utilizes the knowledge of a targeted steganographic technique and may be applicable to such a kind of steganographic method, but may fail on all other steganographic method. But the steganalysis for specific embedding is hardly practical because actually difficult for stegnalyzers to know which steganographic method was used in images.

Universal steganalysis requires no such prior information about which steganographic method was used to hide the data. It can detect the secret message independent of steganographic algorithm. Specific steganalysis method can give more accurate and reliable result than universal approaches, but universal steganalysis is most popular because it can adjust and detect to new or unknown methods.

**1.4.1 Specific Approach**

In specific approach steganalysis techniques are developed to break the particular steganographic method. As Fridrich [2] has proposed attacks on the F5 and Outguess algorithms, both of which work on jpeg images. F5 embeds bits in the DCT coefficients using matrix embedding so that for a given message the number of changes made to the cover image is minimized. But F5 does alter the histogram of DCT coefficients. Fridrich proposes a simple technique to estimate the original histogram so that the number of changes and length of the embedded message could be estimated. The original histogram is simply estimated by cropping the jpeg image by 4 columns and then re-compressing the image using the same quantization table as used before. As is evident in Fig 5, the resulting DCT coefficient histogram would be a very good estimate of the original histogram. Although no analytical proof is given for the estimation method, steganalysis based on this simple technique performs very well.

A second technique proposed by Fridrich [2] deals with the Outguess embedding program. Outguess first embeds information in LSB of the DCT coefficients by making a random walk, leaving some coefficients unchanged. Then it adjusts the remaining coefficient in order to preserve the original histogram of DCT coefficients. Thus the previous steganalysis method where the original histogram is estimated will not be effective. On the other hand when embedding messages in a clean image, noise is introduced in the DCT coefficient, therefore increasing the spatial discontinuities along the 8x8 jpeg blocks. Given a stego image if a message is embedded in the image again there is partial cancellation of changes made to the LSB of DCT coefficients, thus the increase in discontinuities will be smaller. This increase or lack of increase in the discontinuities is used to estimate the message size which is being carried by a stego image.

**1.4.2 Universal Approach**

Universal steganalysis techniques operate by extracting some inherent features of cover image that are likely to modify when an image undergoes steganographic embedding process. Depending on these features/measures classifier is trained and tested for the rest of images. But still these techniques are not performing well for all available steganographic techniques.

The first blind steganalysis method was proposed by Avcibas et al. ref[3] in 2000.this technique used image quality matrics to differentiate between original and stego images. later on techniques based on other features like high order probability density function statistic moments of decomposition subband coefficients[4], center of mask of histogram characteristic function[5],statistical moments of Characteristic function of subband histogram[6], binary similarity measures[7], Steganalysis based on HISTOGRAM and DFT [8] were proposed.

If we do not know about the available steganographic technique used to hide the image then it is called blind image steganalysis. The blind steganalysis attempts to detect steganographic data without knowledge about the steganographic system.

**1.4.1 Structure of blind image steganalysis**

Image blind detection for steganography is actually similar to pattern classification, which centers around two-class classification. Blind detection aims at classifying given images into two categories : cover and stego images. Some existing methods first extract some features from images, then select or design a classifier, and train the classifier using the features extracted from image sets and lastly classify the features. A general structure of blind steganalysis, which consist of three main stages: (1) stego signal estimation; (2) feature extraction; (3) classification. In addition, after extracting features, a feature preprocessing process may be able to enhance the efficiency of classification and its accuracy. Unfortunately, till date there is no detailed framework to describe how to detect images steganography blindly. Here, it is provided more rounded framework of blind steganalysis tentatively, which consists of the following major parts:

1. Image pretreatment: Take some operations for the considered images before feature extracting, such as converting RGB image into grayscale, cropping, JPEG compression, DCT or DWT transformation and so on, to improve the classification performance.
2. Feature extraction: Extract informative features, namely, select the features which are most sensitive to embedding or modification. We should construct the feature vector with low dimension, which will decrease the computational complexity of training and classification.
3. Classifier selection and design: Select or design appropriate classifiers on the basis of extracted features, adopt a large set of images (the classes of images are known) to train classifiers, and obtain some important parameters of classifiers, which will be utilized for the following classification.
4. Classification: Exploit the deduced classifier in (3) to discriminate the given images, and classify them into two categories: stego and original images.

Here, the step of image pretreatment as a part of the process of feature extraction and the structure of blind image steganalysis is shown in **Fig 1.**

**Chapter 2**

**Literature Survey**

Based on the whether an image contains hidden message or not, images can be classified into two classes: one with the hidden message i.e. stego image and other is without hidden message is cover image. Steganalysis can be taken as a task of pattern recognition to decide which class a test image belongs to stego or not. As per the pattern recognition basic task of steganalysis is feature selection. Features should be sensitive to hiding method. In other words we can say features should be different for original cover image and stego image. Larger feature difference means better the feature selection. Features should be general i.e. features should be sensitive all general data hiding methods not to specific method. Often it is very hard to achieve high recognition rate with single feature, so we need to make M-D feature vector. Just like pattern recognition , in addition to feature selection, classifier design is other issue. Both feature selection and classifier design can be evaluate by classification success rate or error rate.

**2.1 Typical Algorithms of feature extraction**

**2.1.1 Image quality metrics**

A good IQM should reflect the distortion on the image well due to, blurring, compression, additive noise and sensor inadequacy. So, a good IQM should be accurate, consistent and monotonic in predicting quality. In 2000 Avcibas et al. [3] conducted a statistical analysis on the sensitivity and consistency behavior of objective IQMs. Twenty six image quality metrics are categorized into six group according to the type of information they use. The measures are categorized into pixel difference, correlation, edge spectrum, context and HVS-based measures. Their sensitivity and consistency to coding as well as additive noise and blur were investigated by analysis of variance(ANOVA). It was found that measures based on HVS, phase spectrum and edge stability measures are most sensitive to coding and blur artifacts, while the mean square error remain the best measures for additive noise.

The selection of IQMs decides the accuracy of detection; however the choice of IQMs in existing references are experimental. In practice, it is hard to choose the optimum one due to the existing large numbers of metrics standard. In addition, selection of multiple measures will increase the implement complexity of feature extraction.

**2.1.2 Higher order PDF moments of subband coefficients**

In 2001 Farid [4] proposed a steganalysis method which exploited statistical regularity of wavelet decompositions. 500 images were collected as database. Three level wavelet decomposition was done. verical, horizontal and diagonal subands at each level were used for furher analysis. For each of these 9 subbands statastics like mean, variance,skewness and kurtosis were obtained. This made total 0f 36 feature vector. The second set of statistics collected were based on the errors in an optimal linear predictor of coefficient magnitude. It was from this error that additional statistics were collected namely mean, variance, skewness and kurtosis to make another 36 –D feature vector. This total of 72-D feature vector was used to differentiate between original and stego images using Fisher Linear Discriminant Analysis. The results were obtained for various steganography methods like Jsteg, EzStego& Outguess. This method provided acceptable results for all the methods.

**2.1.3 COM of histogram characteristic functions**

In 2003 Harmsen and Pearlman [5] began with the fact that data hiding was modeled as additive noise in **Fig. 2.** The stego noise PMF was the distribution of the additive noise, defined as

Equation………6

Where, Is and IC were the pixel values after and before embedding , respectively f[n]is the probability that pixel will be altered by n, n [-255,255]. Let the histogram of stego and cover image hs and hc , respectively. In a hiding system where the additive noise is independent of the cover image, the histogram of stego image equals the convolution of the stego noise PMF and the cover image histogram, and can be described as follows:

Equation………7

So,given a hiding scheme in the form of f[n] and the knowledge of hc[n], the histogram of stego image would be known, where n=0,…,N-1, and N is the largest intensity possible in the image. CF were defined as( DFT of histogram) as follows

Equation………8

DFT of histogramwill be refered as HCF, the formulation of (8) in DFT rewritten as

Equation………9

This shows data embedding will alter the HCF, then the COM of HCF can be expressed as

Equation………10

The COM gave general information about the energy distribution in HCF. Data embedding will result in a decrease in COM, namely

Equation………11

That can be used to differentiate cover from stego images.

To verify the efficiency of this scheme, 24 images from the KODAK digital camera were used, and these images were used, and these images were 24 bit, 768x512 pixels and lossless true color images stored in PNG format. Two detection scheme were built, one against known steganography schemes( SSIS steganography were used) and the against unknown schemes in which SSIS,DCT and LSB steganographic methods were adopted. Although the paper showed that mehod work well, but there only few training and testing images and only 3 steganograhic method were used in experiment. And only full embedding was considered, so performance was desired but it may suffer for law embedding rate.

**2.1.4 CF moments of subband histograms**

In 2005 ref. [6], on each image 2-level Haar wavelet decomposition was performed , so eight subbands denoted by LL1,HL1,LH1,HH1,LL2,HL2,LH2,HH2 and the image itself taken as LL0. For each subband, For each subband, the characteristic function is obtained. That is, we calculate the DFT of the histogram of this subband. Then, the first order moment and the second order moment are extracted according to the following equations:



Where, Aj was the amplitude of the jth frequency components fj.

Which, form an 18-D feature vector for steganalysis. In addition, Bayes classifier and 1096 coreldraw image database were introduced in this paper.In this experiment, 100 images were randomly selected for training, and the remaining 996 images were used for test. For the nonblind cox’s SS. The correct detection rate was 79%; for the blind piva et al’s SS , it is reache 88%, and for the LSB like method, it reached to 91%.

In ref [7], the statistical moments of CF’s from the test image, the prediction-error image and their wavelet subband are combined and select as features. Here the prediction error image is used to erase the image content. Three level HAAR wavelet decomposition done on original image and 1st, 2nd and 3rd order moment calculate for each subband. For each subband calculate prediction error image and find moments for the same, so 78-D feature vectors are used.The Backpropogation Neural Network was used as the classifier. This algorithm is tested against 5 steganographic methods, including cox et al’s non-blind SS(ᾀ=0.1),piva et al’s blind SS, Hung and shi’s block DCT-base SS, a generic QIM(0.1 bpp) and a generic LSB(0.3 bpp) , were used in experiments. It shows the significant performance improvement over Farid and Harmsen. Results of experiment showed that prediction – error images can enhance the changes caused by data hiding through reducing the effects caused by diversity of natural images.

In 2009 Ziwen Sun et.al. Ref[8] has proposed a universal steganalysis method based on characteristic function moment In this method three-level decomposition of image was done. wavelet subbands including the further decomposition coefficients of the first scale diagonal subband. The first three order statistical moments of each band are selected to form a feature vector for steganalysis. The Euclidean distance is used as the separability criterion to analysis the effectiveness of feature vectors for classification and the backpropogation neural network is used as the classifier.

In this method first three moments are calculated for original image and prediction error image, so totally 102-D feature vectors are obtained which was taken as input to ANN classifier. This scheme was tested again Jsteg, Outguess, F5, Jphide, S-tool steganographic method, with powerful detection.

**1.6.5 Binary similarity measure**

Ismail Avcibas Ref [9] develop a steganalysis technique based on binary similarity measure. The basic idea behind this technique was that, the strong correlation between 7th and 8th bit planes as well as the binary texture characteristics within the bit planes will differ if, steganography is applied to an image. This difference was taken as input to SVM classifier to distinguish between stego and cover images.

1800 natural image database was taken for experimental purpose. The steganography algorithms like LSB, LSB +/- where pixel values are incremented or decremented by 1 instead of flipping their least significant bits and JPEG domain algorithms like F5 and Outguess were used.18 different binary similarity measures were obtained for each image to construct 18-D feature vector. These vectors were than used to train and test the SVM classifier.

This method provided better results for LSB like methods compare to method proposed by Farid **ref[4]** in which higher order statistics of wavelet components are used for detecting hidden messages. The Farid methods proved better result for JPEG steganography methods.

**1.6.6 Steganalysis based on HISTOGRAM and DFT :**

In 2009, T. H. Manjuladevi et. al[10] presented a blind steganalysis method using histogram and DFT of an image. 24-D feature vector was obtained and then SVM classifier was used to differentiate between original and stego versions of images. The feature extraction procedure in brief is as mentioned below:

* Separation of the color planesof the color image.
* Build Histogram (*1D*) for each color planes
* Compute the 1st and 2nd moments i.e., mean and variance of the histogram coefficients. This yields *6D* statistics.
* Obtain Discrete Fourier Transform for histogram of each color planes, *c* ∈ *{r, g, b}*. Compute the *1st, 2nd, 3rd and 4th* moments i.e., mean, variance, skewness and kurtosis of the DFT coefficients.
* Compute the total energy for the DFT coefficients. This yields *3D* more statistics.
* The *1st* order moment Mean of the difference of histogram and DFT is computed for each color channel. This yields *3D* statistics.
* This makes total of *24D* features.

This method was tested for steganography method S-Tool. The method provided very good detection rate even for embedding rate less than 5%.

**Classifiers:**

Besides many feature extraction methods of blind steganalysis various classifiers are selected or designed to classify the extracted features. It is well known that different classifiers with the same feature vectors may lead to different detection results. The classifiers used in existing blind steganalysis references almost include all categories of classical classifiers such as FLD, Bayes, ANN and SVM.

**Bayes Classifier[6]**

The notations of w1,*w*2 represent the original image set and the stego image set, respectively.

The mean vectors and covariance matrixes of *w1* and *w2* are represented by µ 1,µ2 and ∑1,∑2 respectively.

The Bayes classification can be stated as

if P(w1|xi) ≥ P(w2|xi),

Xi w1,

Else Xi w2.

Where ,

P(wk|xi) = , k=1,2

**And**  P(xi|w1) = N(xi,µ1,∑1)

P(xi|w2) = N(xi,µ2,∑2) where, N stands for Gaussian Distribution.

**ANN Classifier [7]**

In our work, an artificial neural network (NN) [11], specifically, the feed forward NN with back-propagation training algorithm is used as the classifier. The number of hidden layers is four. All hidden neurons use the tan-sigmoid function. For the one-neuron output layer, all three activation functions (linear, log-sigmoid, tan-sigmoid) have been tested in the simulation. In the training stage, the outputs of log-sigmoid and tan-sigmoid neuron have larger mean square error (MSE) than the linear neuron output. In the testing stage, the linear neuron output provides higher classification rate than the nonlinear outputs. Because log-sigmoid function squeezes the output into the range from 0 to 1 and tan-sigmoid function squeezes the output into the range -1 to 1, more training exemplars or testing patterns may lie on the wrong side at the output. Therefore, a reasonable structure is composed of four tan-sigmoid neuron hidden layers and one linear neuron output layer.

**Chapter 3**

**Implementation and result analysis**

We have implemented several image steganalysis methods and tried to compare the results (success rate and error rate) for well known steganographic algorithms like LSB, spread spectrum method proposed by Cox et. al., Stools and F5.

From the literature survey we came to the conclusion that some steganalysis method, i.e. binary similarity measure based steganalysis[9] is providing very good classification success rate for LSB like methods but, this method is suffering against Non LSB methods i.e. F5 and Cox et. al. The method suggested by Manjuladevi et. al[10] provides excellent results against steganographic method S-tool.We have also observed that among various steganalysis methods “CF moments of subband histograms” based methods provide good classification rate for general blind steganalysis.

**3.1 Implementation Work**

Considering these observation we have implemented steganalysis method based on CF moments of histograms and we have also combined the prediction error to generate feature vectors for training and testing “Naïve Bayes classifier”. We have taken the database of a set of 67 300x225 size original and stego image pairs. We have generated stego database for F5 using VSL tool[11], We have implemented steganographic methods proposed by Cox et. al.[12] and generic LSB to generate stego image database for the same. We have used S-tool [13] for generating S-tool based stego image database.

The implementation steps are mentioned as below:

1. Convert the color RGB image into grayscale image.
2. Perform 2-level wavelet decomposition using HAAR wavelet to get 9 subbands including original image.
3. Calculate histogram of each of the 9 subbands.
4. Calculate DFT of histogram of all the subbands.
5. Find out 1st and 2nd order moments i.e. mean and variance of all the subbands to get

18-D feature vector.

1. Using prediction error image algorithm obtain prediction error image of all the subbands.
2. Now calculate 1st and 2nd order moments of each of these prediction error images to get 18-D feature vector.

This makes total of 36-D feature vector which is used further to train and test the naïve bayes classifier.

We have also tried to get the results by taking 3-level of HAAR wavelet and 3rd moment i.e. skewness as well along with 1st and 2nd order moments. MATLAB 7.6 was used to get the simulation results. The detailed results of all the experiments and discussion on the results is mentioned in next section.

**3.2 Result Analysis**

Different feature vectors taken for experimental purpose:

1. 18- D feature vector ( 1st and 2nd order moments of 9 subbands after 2 level HAAR wavelet decomposition).
2. 36- D feature vector (1st and 2nd order moments of 9 subbands and 9 prediction error images).
3. 52 – D feature vector (1st and 2nd order moments of 13 subbands after 3 level HAAR wavelet decomposition and 13 prediction error images).
4. 78 –D feature vector (1s , 2nd and 3rd order moments of 13 subbands after 3 level HAAR wavelet decomposition and 13 prediction error images).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sr. No. | Feature vector | Cox et. al[ ] | LSB | F5 | S –TOOL |
| 1 | 18 – D |  |  |  |  |
| 2 | 36 – D |  |  |  |  |
| 3 | 52 – D |  |  |  |  |
| 4 | 78 – D |  |  |  |  |

Table 3.1 *Success Classification rate against different steganography methods for various feature vectors.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sr. No | Cox et al [ ] | LSB | F5 | S-TOOL |
| Ferid [] |  |  |  |  |
| Binary similarity measures[] |  |  |  |  |
| 2009 [ ] |  |  |  |  |
| Our design [ ] |  |  |  |  |

Table 3.2 *Comparison results of our algorithm with other steganography methods*

ADFAFSADADFAFD—DF-SADF-SA-D-FA-DF-A-D--

**Chapter 4**

**Problem Definition**

**References**

[1] T. Morkel, J.H.P. Eloff , M.S. Olivier “An overview of image steganography.” Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[2] J. Fridrich, M. Goljan, D. Hogea, and D. Soukal, “Quantitive steganalysis of digital images: Estimating the secret message lenght,” *ACM Multimedia Systems Journal,Special issue on Multimedia Security*, 2003.

[3] I. Avcibas, N. Memon, B. Sankur, Steganalysis of watermarking techniques using image quality metrics, in: Proceedings of the SPIE,Security and Watermarking of Multimedia Contents II, vol. 4314,2000, pp. 523–531.

[4] H. Farid, Detecting steganographic messages in digital images,Technical Report TR2001-412, Dartmouth College, Hanover, NH,2001.

[5] J.J. Harmsen, W.A. Pearlman, Steganalysis of additive noise modelable information hiding, in: Proceedings of the SPIE, Security,Steganography, and Watermarking of Multimedia Contents V,vol. 5020, 2003, pp. 131–142.

[6] Y.Q. Shi, G.R. Xuan, C.Y. Yang, J.J. Gao, Z.P. Zhang, P.Q. Chai, D.K. Zou,C.H. Chen, W. Chen, Effective steganalysis based on statistical moments of wavelet characteristic function, in: Proceedings of IEEE International Conference on Information Technology: Coding and Computing, 2005, pp. 768–773.

[7] Y.Q. Shi, G.R. Xuan, D.K. Zou, Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network, in: Proceedings of IEEE International Conference on Multimedia and Expo, 2005, pp. 269–272.

[8] Ziwen Sun, Hui Li, Zhijian Wu, Zhiping Zhou,  **A Image Steganalysis Method Based on Characteristic Function Moments of Wavelet Subbands ,** in: Proceedings of IEEE International Conference on Artificial Intelligence and Computational Intelligence, 2009

[9] ˙Ismail Avcıbas¸ Mehdi Kharrazi, NasirMemon, B¨ulent Sankur, Image Steganalysis with Binary Similarity Measures, EURASIP Journal on Applied Signal Processing 2005:17, 2749–2757 © 2005 Hindawi Publishing Corporation.

[10] T. H. Manjula Devi1, H.S.Manjunatha Reddy,2 K. B. Raja3Venugopal K. R3 and L. M. Patnaik4, Detecting Original Image Using Histogram, DFT and SVM International Journal of Recent Trends in Engineering Vol. 1, No. 1, May 2009.

[11] http://vsl.sourceforge.net/

[12] I.J. Cox, J. Kilian, T. Leighton, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Trans. Image Process. 6 (12) (1997) 1673–1687.

[13] A. Brown, S-tools version 4.0. [Online]. Available: http://members.tripod.com/steganography/stego/s-tools4.htmlS.