ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

A Review on Digital Image Steganalysis Techniques Categorised by Features Extracted

Rita Chhikara, Latika Singh
ITM University, Gurgaon, Haryana, India

Abstract- The overwhelming growth in communication technology and usage of public domain channels (i.e. Internet) has greatly facilitated transfer of data. However, such open communication channels have greater vulnerability to security threats causing unauthorized information access. Steganography is the art of hiding and transmitting data through apparently innocuous carriers such as text, image, audio or video in an effort to conceal the existence of the secret data and the fact that communication is even taking place. Steganalysis is an attack on steganography. Both steganography and steganalysis have received a great deal of attention from law enforcement and the media. In the past years many powerful and robust methods of steganography and steganalysis have been reported in the literature. In this paper, we classify and give an account of the various approaches that have been proposed for steganalysis. Some promising methods for universal steganalysis with respect to features and classification techniques have also been identified.

Index Terms: **Steganography, Steganalysis, DCT, DWT, Spatial domain, SVM, ANN, ANOVA, PSO.**

I. INTRODUCTION

Steganography is the science of embedding hidden messages in the cover multimedia i.e text, images, audio, video files [1]. A lot of steganographic tools are today freely available on the internet such as EZ Stego[2], J-Steg[2], JPHide&Seek[2], Outguess[2], F5[3] etc. Most of the steganographic methods modify the redundant bits in the cover medium (carrier) to hide the secret messages which changes the statistical properties of cover medium to create a stego medium. The most widely used image steganographic techniques are substitution technique in (i) Spatial Domain[4][5] (ii) Transform domain[6] like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) (iii) Spread spectrum technique[7]. A survey of all these techniques is given by Petitcolas and Anderson [8]. As any modern communication technology, steganography can be misused by criminals for planning and coordinating criminal activities. By embedding messages in images and posting them on binary newsgroups or public sites, it is difficult to discover the communication act itself and trace the recipient of the message. Thus the concern is to lessen these negative effects by developing the techniques of steganalysis. Steganalysis is science of breaking steganography. The goal of steganalysis is to collect sufficient evidence from observed data to discriminate a carrier as 'stego' or 'cover' based on presence or absence of embedded message. Images are often used as a carrier because of their extensive availability with high resolution of pixels. Data embedding in a multimedia carrier like image may involve varying parameters such as different image formats, different embedding algorithms and various steganographic keys. This has made steganalysis a more difficult and challenging task. Earliest work on steganalysis was reported by Johnson and Jajodia [9] and Chandramouli et al.[10]. It has gained prominence in national security and forensic sciences as detection of hidden messages can lead to the prevention of disastrous security incidents. Algorithms for Steganalysis are primarily of two types : (i) Specific or targeted: The Specific approach represents a class of image steganalysis techniques that very much depend on the underlying steganographic algorithm used and have a high success rate for detecting the presence of the secret message. (ii) Generic: The generic steganalysis algorithms usually referred to as universal or Blind Steganalysis algorithms, work well on all known and unknown steganography algorithms. It can be considered as a two class pattern classification problem. In the training phase set of features such as markov features, dct coefficient feature set, wavelet coefficient features etc. of both stego and cover images are provided to a statistical classifier. The learning classifier determines the best classification rule using these images. In the testing phase same set of features of unknown images are given as input to the trained classifier to decide whether image contains a secret message or not and hence discriminate it as stego or cover. The universal steg analysis algorithms are usually less accurate than targeted ones, but a lot more expandable. In this paper an attempt has been made to make a note of the various approaches proposed for the steganalysis of digital images and classify them based on features extracted. The performance of these techniques as evaluated in these papers has also been given. Finally, the most promising steganalytic techniques have been identified. The rest of the paper is organized as follows. In Section 2 the specific steganalysis techniques categorized on spatial and transform domain is given. Section 3 deals with universal steganalysis techniques. Summary and conclusions drawn from the study have been given in Section 4.

II. SPECIFIC STEGANALYSIS TECHNIQUES

These methods target a particular steganographic embedding algorithm. These techniques try to analyze the

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

image for finding the embedded message and concentrate on some image feature or statistics which are modified by that embedding algorithm.

A. Signature Steganalysis

Steganography methods hide secret information and manipulate the images and other digital media in ways as to remain imperceptible to human eye. But hiding information within any electronic media using steganography requires alterations of the media properties that may introduce some form of degradation or unusual characteristics and patterns. These patterns and characteristics may act as signatures that broadcast the existence of embedded message In[11] signature based attacks are adopted to detect the presence of hidden messages. It is reported that Jpegx, a data insertion steganography stool, inserts the secret message at the end of JPEG files marker and adds a fixed signature of the program before the secret message. The signature is the following hex code: 5B 3B 31 53 00. The presence of this signature automatically implies that the image contains a secret message embedded essentially using Jpegx.

B. Specific Statistical steganalysis

Steganography embeds secret messages in images, this causes alterations in the statistics of an image. Statistical steganalysis, as the name implies, analyses this underlying statistics of an image to detect the secret embedded information. Statistical steganalysis is considered powerful than signature steganalysis because mathematical techniques are more sensitive than visual perception. Specific statistical steganalysis can be classified based on data hiding techniques i.e in spatial domain and transform domain.

i) Spatial domain steganalysis

a) Chisquare Attack

The first ever statistical steganalysis was proposed by Westfeld and Pfitzmann[12]. This approach is specific to LSB embedding and is based on powerful first order statistical analysis rather than visual inspection. The technique identifies Pairs of Values (POVs) which consist of pixel values, quantized DCT coefficients or palette indices that get mapped to one another on LSB flipping. After message embedding, the total number of occurrence of two members of certain POV remains same. This concept of pair wise dependencies is exploited to design a statistical Chi-square test to detect the hidden messages[12][13]. The reported results show that this method reliably detects sequentially embedded messages. Later, the method was generalized to detect randomly scattered messages [14].

b) RQP (Raw Quick Pair)

Another specific steganalytic method for detecting LSB embedding in 24-bit colour images—the Raw Quick Pair (RQP) method is proposed by Fridrich et al.[15]. The method is based on analyzing close pairs of colours created by LSB embedding. It has been shown that the ratio of close colours to the total number of unique colours increases significantly when a message of a selected length is embedded in a cover image rather than in a stego image. It is this difference that enables to distinguish between cover images and stego images for the case of LSB steganography. The method works reliably well as long as the number of unique colours in the cover image is less than 30% of the number of pixels. As reported the method has higher detection rate than the method given by Westfeld and Pfitzmann[12] but cannot be applied to grayscale images.

c) RS Steganalysis

A more sophisticated technique RS steganalysis (Regular and Singular group) is presented by Fridrich et al[16] for detection of LSB embedding in colour and grayscale images. This technique utilizes sensitive dual statistics derived from spatial correlations in images. The image is divided into disjoint groups of fixed shape. Within each group noise is measured by the mean absolute value of the differences between adjacent pixels.

Each group is classified as “regular” or “singular” depending on whether the pixel noise within the group is increased or after flipping the LSBs of a fixed set of pixels within each group using a “mask”. The classification is repeated for a dual type of flipping. Theoretical analysis and experimentation show that the proportion of regular and singular groups form curves quadratic in the amount of message embedded by the LSB method. RS steganalysis is more reliable than Chi-square method [12].

d) B-Spline fitting

Shunquan Tan and Bin Li[74] claims that there is no targeted steganalysis against EALSBMR. They proposed that B-Spline can be used to fit the histogram to remove the pulse distortion caused by readjusting phase of EALSBMR. This method can accurately estimate the threshold used in the secret data embedding procedure and separate the stego images with unit block size from those with block sizes greater than 1.

ii) Transform domain steganalysis

a) Chi-square statistics

Zhang and Ping[17] have proposed an attack on sequential JSteg and random JSteg for JPEG images. The technique is based on the statistical model of DCT coefficients. It is observed that the quantized DCT coefficients of JPEG images distribute symmetrically around zero in clean images. These distributions are changed owing to the message embedding; sequential or random. Chi-square statistics of stego image are calculated and an inequality equation is used to judge the presence of hidden message. The embedding ratio is also calculated. The technique is simple and very effective.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

b) Histogram Analysis Attack

Histograms analysis attack works on JPEG sequential and pseudo-random embedding type stegosystems, such as JSteg and Outguess 0.1. It can effectively estimate the length of the message embedded and it is based on the loss of histogram symmetry after embedding. X. Yu et al[18] proposed a powerful steganalysis method specific for JSteg steganography in JPEG file format. In this technique the cover image histogram of DCT coefficients is estimated from the stego image histogram. This estimation is more accurate than Fridrichs cropping method.

c) Calibration Technique

Fridrich [19] proposes a feature-based steganalytic method which is combined with the concept of calibration for JPEG images. First and second order features are analysed both in DCT and spatial domain like global DCT coefficient histogram, dual histograms, blockiness, co-occurrence matrix. In order to estimate the cover image we take into account how JPEG works. Based on the fact that JPEG images have a block structure of 8x8 blocks and are formed by quantized DCT coefficients, which tend to be robust to small distortions such as compression and embedding, we can estimate the cover image. Thus, by decompressing and recompressing an image with different block structure we can estimate the cover image. This is done by using the following calibration technique on the stego image.

- Decompress the stego image using its quantization table.
- Crop the decompressed stego image by 4 pixels, either column-wise or row-wise or at the edges.
- Compress the cropped image using the same quantization table.

III. UNIVERSAL STEGANALYSIS

Specific steganalytic techniques yield accurate decisions when tested only on that method and may fail if any other steganographic technique is used. Universal steganalysis overcomes the deficiency of specific steganalysis techniques. Universal Steganalysis can be considered as a two-class pattern classification problem to classify the test image as either a cover or a stego image. Generally, the classification consists of two parts, feature extraction and pattern classification. Since image data is typically very large, a lower dimensional representation of the information in the image, relative to the classification task at hand, is required. A feature is such a lower-dimensional representation of the image data and is crucial for many classification problems, including steganalysis. The best features for steganalysis should contain information about the changes incurred by data hiding rather than by the content of the image. Survey based on various features extracted is given below.

A. Markov Features

A steganalysis method by Shi and Chen[20] uses Markov empirical transition matrices to capture both intra-block and inter-block dependencies between block DCT coefficients in JPEG images. Features are extracted from empirical transition matrices by a threshold technique. These features are evaluated with SVM. Zou, Shi and Xuan[21] extracted the markov features from prediction-error image. Image pixels are predicted with their neighbouring pixels. The prediction error is obtained by subtracting the prediction values from the pixel value and then thresholded with a predefined threshold. For feature classification, the SVM with both linear and non-linear kernels are used as classifier. The non-linear SVM performs much better than linear SVM for proposed higher-dimensional features. It has been reported by the author that the results are more effective than Fridrich's[19]. Markov features are further extended by Wing and Zhi-Min [73] to original, difference and second difference JPEG arrays. The Markov features based on the original JPEG array capture the characteristics of the distribution of DCT coefficients while Markov feature based on difference and second difference JPEG arrays capture differences among neighbouring coefficients. According to author these three merged Markov features improves the performance of steganalysis system. RBFNN (Radial Basis Neural network) is used as a classifier. The experimental results in the paper show that the generalization capability for different image database of proposed method outperforms the methods of Fridrich [19] and Shi and Chen[20]. Penvy and Fridrich[22] presents a method for detection of steganographic methods that embed in the spatial domain by adding a low-amplitude independent stego signal, an example of which is least significant bit (LSB) matching. SPAM(Subtractive Pixel Adjacency Matrix) features are formed by the average sample Markov transition probability matrices and steganalyzer is implemented by support vector machines. The comparison to prior art reveals that the presented feature set offers superior accuracy in detecting LSB matching. Even though the feature set was developed specifically for spatial domain steganalysis, by constructing steganalyzers for ten algorithms for JPEG images, it is demonstrated that the features detect steganography in the transform domain as well.

B. Image Quality Metrics

Memon and co-workers [28] have demonstrated that the steganographic schemes leave statistical evidence that can be exploited for detection with the aid of image quality metrics and multivariate regression analysis. Distance in the feature space between an unmarked and a reference image is different than the distance between a marked image and its reference version. Around 26 image quality metrics are used as the feature set. To identify good features (quality measures), which provide the best discriminative power, ANOVA technique is used.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

C. Wavelet Transform Features

Minh and Martin[25] extracted wavelet coefficients in each sub-band of wavelet transform and modelled them as a Generalized Gaussian Distribution (GGD) with two parameters, viz., shape and scale. These parameters are good measure of image features in[26] and are used to discriminate between stego images from innocent images. Neural network is adopted to train these parameters to get the inherent characteristics of innocent and stego images The universal steganalytic technique proposed by Farid[29] uses a different approach for feature extraction from grayscale images. The decomposition employed is based on separable quadrature mirror filters (QMFs). A statistical model is build which is composed of mean, variance, kurtosis, skew of sub-band coefficients and error statistics from an optimal linear predictor of coefficient magnitudes. A Fisher Linear Discriminant analysis is then used to discriminate between untouched and adulterated images. Lyu and Farid[30] extended the statistical model to first and higher order colour wavelet statistics. A one-class support vector machine (OC-SVM) is employed for detection of secret messages in digital images. Lyu and Farid[31] further extended the statistical model to include phase statistics in addition to first and higher order magnitude statistics to extract 432-D feature vector. The experiments and results show that this method is more reliable in detecting steganography. A steganalysis technique based on multiple features is given by Xuan et al[33]. He extracted 39-D feature vectors from statistical moments of wavelet characteristic functions and adopted Bayes classifier to classify the testing images. Wen-Nung and Guo-Siang[32] proposed a set of two image features; the gradient energy and the statistical variance of the Laplacian parameters. The proposed system is effective in detecting any steganography embedding technique and has been shown to give 90% positive detection rate. Y.Wang and P.Moulin[34] made an effort in wavelet decomposition, re-decomposing the diagonal sub band on first scale. This paper compared the PDF moments given by Lyu and Farid[31] with CF moments given by Xuan et al[33] and indicated that for wavelet subbands, the CF moments are more sensitive to hidden message than PDF moments , while for prediction error subbands , PDF moments would be better. Results of experiment showed that this method works better in LSB, SSIS and F5 steganography. Usefulness of a feature is evaluated with Bhattacharya distance measure and FLD classifier is adopted for training and testing. Xiangyang Luo, Fenlin Liu[36] computed the features from the characteristic functions of subbands of transform domains, such as the wavelet coefficient subbands, the prediction subbands of wavelet coefficients, the prediction error subbands of wavelet coefficients, the wavelet coefficient subbands of image noise, and the log prediction error subbands of wavelet coefficients. CF have been shown experimentally by Wang and Moulin [34] to be more sensitive to embedded message than PDF. Classification is performed with FLD (Fisher Linear Discrimination) and SVM (Support Vector Machine). For a given gray scale image Shuang - Huan Zhan and Hong-Bin Zhang[38] performed four-order discrete 2-D wavelet decomposition to capture statistical model based on mean, variance, skewness and kurtosis to obtain 36-D feature vector. Another set of 36 elements were obtained from log error statistics of an optimal linear predictor. All 72 elements were further processed by ANOVA (Analysis of variance) to find the sensitivity of these wavelet statistics to hidden message. Steghide, Hide4pgp and S-tools are used to hide message in images. Compared to Farid's[29] method testing rate based on ANOVA showed improvement. Gireesh and Jithin[52] extracted features from statistical model of all three channels of image that is red, green and blue after wavelet decomposition based on separable Quadrature Mirror Filter (QMF) to get 108 features and classified using SVM. Guoming Chen, Qiang Chen[47] decomposed a test image using a three-level Haar transform, resulting in 13 subbands in total. For each subband, they derived first three moments of characteristic functions resulting in a set of 39 features and another set of 39 features from prediction-error. Author reduced the features by PSO (Particle Swarm Optimization), which is a random population searching optimization algorithm. It works on the concept that each single candidate solution is a particle in the search space and each particle makes use of its individual memory gained by the swarm as a whole to find the best solution. The accuracy of classification trained by Support vector machine and corresponding selected features are used as fitness function for optimization. The author proves through experimental result that detection rate increases from 5% to 8% when PSO is applied. The proposed method[53] takes 1-level wavelet decomposition of the image with Haar QMF and divides it in horizontal, vertical and diagonal subbands into overlapping windows. It then constructs an over determined equation system for each window which is solved using Moore-Penrose pseudo-inverse of matrix. Thereafter a linear predictor error for all sub-bands is calculated. The features are extracted from the error vectors obtained from the sub-bands and classified using Linear Support Vector Machine. The experiments confirm that this method is superior to Lyu's[31] and Glojan's method[54]. Xiangyang Luo and Fenlin Liu[48] firstly, decompose image into three scales through WPT (wavelet packet transformation) to obtain 85 coefficient sub bands together, and extract the multi-order absolute characteristic function moments of histogram from them as features. And then, normalize these features and combine them to a 255-D feature vector for each image. They adopt a back-propagation (BP) neural network to classify cover and stego images. This method has higher average detection accuracy compared to Xuan et al[33] and Wang method[34] as indicated by experiment results.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

Ziwen Sun and Hui Li[49] also classifies using BP neural network on features extracted from characteristic function moments of three-level wavelet sub bands including the further decomposition coefficients of the first scale diagonal sub band. He extends his work by analysing effectiveness of feature vectors using the Euclidean distance to get better performance. Li Hui, Sun Ziwen[50] utilizes PCA (Principal component analysis) to reduce the features and SVM is adopted as classifier. The detection accuracy improves with reduced feature set.

D. Co-occurrence Matrix

Kodovsky[39] designed 7850-dimensional features that are produced from the co-occurrence matrices of DCT coefficient pairs and called as CF* features. Since both the intra-block and inter-block dependencies are represented by the features, the steganalytic method can effectively detect the hidden data in JPEG images. An ensemble classifier mechanism is presented to solve the problem, in which the individual Fisher Linear Discrimination (FLD) classifiers are trained in a random feature subspaces with low dimensions, and the final decision on a suspicious medium is made by fusing the individual FLD decisions with majority voting strategy. This way, both the good classification performance and the satisfactory computational complexity are ensured. The steganalystic scheme by Fengyong Li and Xinpeng Zhang [40] is comprised of two parts : feature extraction and Bayesian ensemble classifier. The features are extracted in two parts: one part is generated from the coefficient co-occurrence matrices, which are 7850 features proposed by Kodovsky[39], while another part is derived from the co-occurrence matrices of coefficient differences. Cartesian calibration method is used to produce other 7850 features; hence a total of 15700 high dimensional feature set is used for steganalysis. The extracted features firstly are to used train a number of sub-classifiers, which are integrated as an ensemble classifier with a Bayesian mechanism. In construction of each sub classifier *d* features from 15700 are used to train FLD (Fisher linear discriminate) classifier. Around 201 sub classifiers are obtained with different subset of features. Embedding method employed is nsF5 and Model based steganography. Merging the two features improves performance by 2%. Ziwen Sun and Maomao Hui[62] calculates the forward difference in three directions, horizontal, vertical and diagonal, towards adjacent pixels to obtain three-directional differential images for a natural image. Then the differential images are thresholded with a pre-set threshold to remove the redundant information. The co-occurrence matrixes of thresholded differential images are used as features for steganalysis. The performance of this method is evaluated on 3 steganographic methods Cox's Spread Spectrum (SS), +-1 method and generic LSB's with data embedding rate of 0.3, 0.2 and 0.1 bpp resp. Support vector machine (SVM) with RBF kernel are applied as classifier.

E. Histogram Features

Kodovsky[37] proposed that JPEG-compatibility steganalysis detects the presence of embedding changes using the fact that the stego image was previously JPEG compressed. The difference between the stego image and an estimate of the cover image is calculated. The cover image is obtained by recompression with a JPEG quantization table which is estimated from the stego image. The recompression arti-facts are described using a 65-dimensional feature vector formed as the histogram of blocks with a certain number of mismatched pixels. Ensemble classifiers are built to assess the detection accuracy for a fixed embedding change rate, a constant false-alarm rate detector for an unknown change rate, and a quantitative detector. The proposed approach offers significantly more accurate detection even for very small change rates. The technique requires an accurate estimate of the JPEG compression parameters. Deng Qian-lan[61] proposed a feature vector as 18 2-D histograms obtained from a given color image, 9 are the 2-D adjacency histogram of the three direction differential image and the other 9 are the 2-D histograms among the differential images of three color plane. They then calculated the 2-D DFT histograms resulting in a set of 54 features. Support vector machine with RBF kernel is applied as classifier. Deng Qian-lan[68] further extracted features from the DFT of the histogram of differential image. Four histograms are obtained from a given image , 1 from the histogram of image itself and 3 histograms of the difference in three directions, horizontal, vertical and diagonal towards adjacent pixels to obtain three-directional differential images for a natural image. The features are then divided into low and high frequency bands. Support vector machine (SVM) with RBF kernel is applied as classifier. The run length features proposed by Dong and Tan[63] uses the histogram characteristic function. They take the first three HCF moments for each histogram. Using three different images; quantised, difference and original and four directions; horizontal, vertical, minor and major diagonals, they get a 36-D feature vector which outperforms [64] and [65].

F. Binary Similarity Measure

Avcibas[66] assumed that any steganographic manipulation on an image will alter the patterns in the neighbourhood of a bit in its bit plane as well as across the bit planes. So he inspected the similarity measure between two successive binary images. With 18 features obtained from images he used SVM classifier. The comparative experiments with LSB, LSB+/-, F5 and Outguess +/- embedding techniques proved Avicabas's method to be superior for LSB and LSB +/- while Farid's method[29] was superior in case of F5 and Outguess. Jing-Qu Lin; Shang-Ping Zhong[69] captured the seventh and eighth bit planes of the non-zero DCT coefficients from JPEG images as opposed to bit planes in Avcibas's method[66] which are derived from spatial domain. 14

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

features of each image based on binary similarity measures are computed. C- Support Vector Classification and RBF kernel function is used for classification. This method has close detecting accuracy compared to Fridrich's [19] method, but average time is 25 times faster than[19] as no calibration image is generated.

G. Contourlet Transform Features

The contourlet transform is an extension to the wavelet transform in two dimensions using nonseparable and directional filter banks. It is composed of basis images oriented at varying directions in multiple scales. With this rich set of basis images, the contour let transform can effectively capture the smooth contours in the natural texture images. Contourlet representation can also extract the intrinsic geometrical structures in the textural images which wavelets fail to capture. Sajedi and Mansour [55] considered the statistical moments of contourlet coefficients in each subband as the first feature set. Using the linear predictor as applied by Farid[31], the author computed the log error between the actual coefficient and the predicted coefficient magnitudes and the first four moments of differences are considered as the second feature set. They performed experimental results on powerful steganography methods, such as , model based (MB) [75], perturbed quantization (PQ) [76], and YASS [77]. The method showed effectiveness in comparison to previous famous steganalyzers given by Farid[31] and Fridrich[19]. Steganalysis based on the features that are obtained from contourlet transformation was proposed by Sheikhan, M., Moin[78]. The extracted features are statistical moments i.e. mean, variance, skewness and kurtosis and co-occurrence statistics like angular second moment, homogeneity, contrast and correlation of contourlet coefficients. Also the linear prediction of magnitude coefficients is performed and statistical moments of log error between actual and linear predicted coefficients of contourlet transform are used as the features. The usefulness of feature is evaluated by Analysis of Variance (ANOVA) technique. It selected 102 features from 1728 features extracted from Contourlet transformation in 3 scales and 8 directions and 3 colour channels. SVM is used to detect accuracy of this system.

H. Merged Features

The data hiding techniques used by S. Liu et al.[23] were quantization index modulation methods, DWT middle frequency pair (MFP) and adaptive based technique. For steganalysis they did quantitative analysis of image features with hidden messages spectrum analysis and energy differences to score for differences in the histograms of cover and stego images. The experimental results were reported to be accurate. A neural network based steganalysis is given by Shaohui Liu and Yao Hongnun[24]. The digital images, cover as well as stego, are analysed in DCT, DFT and DWT transform domains using neural network. Results indicate that the method is promising. Penvy and Fridrich [35] proposed a new set of features for steganalysis of JPEG images which is obtained by merging 193 DCT feature set that captures inter-block dependencies among DCT coefficients and Markov features which capture intra-block dependencies. Calibration is applied to Markov features and their dimensionality is further reduced by a factor of 4 hence obtaining 81 Markov features. The resulting feature sets are merged, producing a 274-dimensional feature vector. The new feature set is then used to construct a Support Vector Machine multi-classifier capable of assigning stego images to six popular steganographic algorithms—F5, OutGuess, Model Based Steganography without , and with deblocking, JP Hide&Seek, and Steghide. The new feature set provides significantly more reliable results however the images undergoing double compression have a high probability of misclassification. Yoan Miche, Patrick Bas and Amaury Lendasse[41] presented a methodology for steganalysis based on a set of 193 features proposed by Penvy and Fridrich[35] with two main goals: to determine a sufficient number of images for effective training of a classifier and use feature selection to select most relevant features for the desired classification. These 193 features consider statistics of JPEG compressed images such as histograms of DCT coefficients for different frequencies, histograms of DCT coefficients for different values, global histograms, blockiness measures and co-occurrence measures. Author uses Outguess algorithm for embedding messages into images as it is able to resist statistical attack. By the use of a Monte-Carlo technique on up to 4000 images, it has been shown that such numbers of images are sufficient for stable results. A SVM (Support Vector Machine) is finally used on reduced feature set, 13-D feature vector to classify images as stego or cover. Performance is comparable with 193-D feature set. Q. Liu, A. H. Sung and Z. Chen[42] has extracted the following five types of features for gray scale steganalysis : Shape parameter of the GGD (Generalized Gaussian Distribution) of the HH wavelet sub-band that measures the image complexity, Entropy of the histogram of the nearest neighbors, the high-order statistics of the histogram of the nearest neighbors PEN (Probabilities of the equal neighbors), Correlations features . In comparison with other well-known feature sets, the set of proposed features performs the best.. The combination of a dynamic evolving neural fuzzy inference system (DENFIS) with a feature selection of support vector machine recursive feature elimination (SVMRFE) to classify the images as stego or cover. It achieves the best detection performance when compared with the following classifiers: naive Bayes classifier (NBC), support vector machines (SVM), quadratic Bayes normal classifier (QDC), and adaboost. Y. Miche and P. Bas[43] use a wrapper-type method to reduce the number of features for JPEG steganalysis. Bootstrap simulations are used for classification on minimum 5000 images in order to perform reliable steganalysis. Feature selection is performed using OP-ELM (Optimally-Pruned Extreme

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

Learning Machine) classifier. This enables both to reduce the dimensionality of the data and to highlight weaknesses and advantages of the six most popular steganographic algorithms. G.K. Rajput and R.K. Agrawal[44] use filter as well as wrapper method to evaluate the performance of steganalysis. Kullback divergence measure, chernoff distance measure and linear regression are used for relevant feature selection. The performance of steganalysis using different measures used for feature selection is compared and evaluated in terms of classification error and computation time of training classifier. A Linear Discriminant Analysis is used for classification. Experimental results show that Linear regression measure used for feature selection outperforms other measures used for feature selection in terms of both classification error and compilation time. Gaurav Rajput, R.K. Agrawal[45] exponential discriminant analysis, a variant of linear discriminant analysis (LDA), is proposed which transforms the scatter matrices to a new space by distance diffusion mapping. This provides exponential discriminant analysis (EDA) much more discriminant power to classify non-linearly separable data and helps in improving classification accuracy in comparison to LDA.

Features for steganalysis are obtained from statistics of the histogram, wavelet statistics, amplitudes of local extreme from the 1D and 2D adjacency histograms, center of mass of the histogram characteristic function and co-occurrence matrices by Mahdi Ramezani and Shahrokh[46]. In order to reduce the proposed features dimension and select the best subset, they use genetic algorithm and the results are compared through principal component analysis and linear discriminant analysis. The performance of classification methods based on Fisher Linear Discriminant, Gaussian naïve Bayes, multilayer perceptron, and k nearest neighbor are compared on features extracted. To study the effect of the GA-based feature selection, the classification error of the FLD classifier is chosen as the fitness function. They found the method to be reliable even for large feature set. Yuan-lu Tu; Sheng- rong Gong[56] converted the images to YUV color space to separate the luminance and chrominance components. This overcomes the fault that neglects the inherent correlation between RGB channels. Double domain features variance of scale factor of Laplacian distribution of DCT coefficients macro-block and moment of characteristic function in DWT domain which are more sensitive to steganography as given by Lyu and Farid[30] are extracted. SVM is employed to map data into a high dimensional space and finding a separating hyper plane with maximal margin. The method outperforms chen's method [51]. Zhuo Li, Kuijun Lu, Xianting Zeng, Xuezeng Pan[57] combine the concepts of image calibration[19] and COM (centre of mass) of HCF (Histogram Characteristic Function) to collect thirteen statistics in the DCT domain and spatial domain, 82-dimensional feature vector for each image is calculated by using the characteristic function and the COM for each statistic. Support vector function (SVM) is utilized to construct the blind classifier. It outperforms Shi et al[65] when spread spectrum steganography method Cox is used. It also gives comparable result with their method when F5, Jsteg, Jphide & seek, Outguess and Steghide is used for embedding. Wenqiong Yu; Zhuo Li; Lingdi Ping[58] proposed an SADRID-I image steganalysis algorithm that is based on improved differential matrix, according to the high dimensions and correlation of image features. It reduces features dimensions using rough set theory. It was tested on 324 D feature[72] extracted from DCT domain, wavelet domain and space domain in JPEG images and Shi's[65] 78 features, which showed efficiency in time, space and accuracy in detection after features were reduced. SVM is applied as a classifier. Cai Hong and S.S Agaian[59] present an algorithm for detecting the secret message embedded by F5 algorithm. The extracted spatial and DCT domain features are concatenated to construct a new fusion feature. This method monitors the fusion feature changes derived by blocking artifacts due to embedding hidden message. The results demonstrate an effective attack to F5 even with very low embedding rates and assured low false-positives. Wenqiong Yu; lly hZhuo Li; Lingdi Ping[60] argues that JPEG steganography methods such as JPhide, Outguess etc. always embed the secret messages by manipulating the quantized DCT coefficients. Therefore the features constructed in DCT domain may lead to be more sensitive to the embedding changes. Hence in this paper he constructs nine statistical models from the DCT and decompressed spatial domain for a JPEG image and by calculating the histogram characteristic function (HCF) and the center of mass (COM), the energy distribution of each model as one part of the feature set is measured. Support vector machines are utilized to construct classifiers. This method performs better detection accuracy with low as well as high embedding rate when compared with Fridrich's [19]and Shi's method[20]. Pevny and Fridrich [67] author works with only stego images and a set of steganographic features , 274-PEV features[35]. Regression tolls linear least square regression and a kernelized variation called support vector regression are used to learn the relationship between the features location and number of embedding changes. Shaohui Liu; Lin Ma; Hongxun Yao; Debin Zhao[70] showed that proper reorganization of block based DCT coefficients can have similar characteristics to wavelet transforms. The test and the predicted-error images are decomposed using block-based DCT to generate 228 features. SVM is used as a classifier because of its comparable and efficient classification performance. They have embedded data using LSB (Least Significant Bit), QIM(Quantization Index Modulation) and SS(Spread Spectrum) technique. The method outperforms Farid's[29] and Xuan's method[33]. Hong Zhao and Hongxia[71] proposed a blind steganalysis for detecting GIF steganographic

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

algorithms. They generated features from generalized difference images and color correlogram and found them to be highly effective in discriminating stego images from cover images, since these features captured the correlations between adjacent pixels. The features were classified with SVM using Radial Basis Function and author shows through results that the proposed method outperforms Fridrich's[19] and Lyu's method[31] when embedding rate is above 20%. However the method is not very effective for adaptive steganography. Xiang Yang and Zhang Wen-hua[80] presents a steganalysis method of lower dimensional feature set. They calculate 198-dimensional feature vector in the wavelet domain as statistical moments of wavelet characteristic function and markov process features of low frequency coefficients. A SVM with RBF is used as a classifier. It provides better results than Kodovsky[79] for detecting YASS(Yet Another Steganographic Scheme). This method includes a 686-dimensional feature set SPAM (Subtractive Pixel Adjacency Matrix) and Cartesian calibrated 548-D feature set extracted mainly from quantized DCT coefficients.

IV. SUMMARY AND CONCLUSION

In this paper we have given an overview of various steganalytic techniques for digital images. The techniques are broadly classified as specific and universal steganalysis. They are further categorised based on features being used for discriminating the images as stego or cover. From the study of methods reported in this paper we infer that the results from most Specific statisticalsteganalysis techniques[14][15][16][17][18][74] are very accurate and give better results than signature analysis[11] , but these techniques are inflexible since most of the time there is no path to extend them to other embedding algorithms. Universal statistical steganalysis are more robust as they are designed to detect messages embedded using any steganographic technique and without the knowledge of embedding technique. In this paper we have categorised the study based on various features extracted and it has been found that features extracted from wavelet coefficients give better result than spatial domain or DCT(Discrete Cosine Transformation) coefficients as correlation capability of DWT(Discrete Wavelet Transformation) coefficient[30][31][33] of each sub band at same level are independent hence features generated are independent of each other, which is suitable for steganalysis. Moments of Characteristic Function of wavelet coefficients [34][36][47][48][49][50] provide better efficiency. It can further be inferred from the study that the contourlet transform[55][78] can effectively capture the smooth contours in the natural texture images and can also extract the intrinsic geometrical structures in the textural images which wavelets fail to capture, hence gives better detection accuracy than features extracted from wavelet coefficients. However the detection accuracy improves when combination of these features extracted from spatial domain and frequency domain (DCT, DWT) is used as is shown by study in section 3.8 (mergedfeatures)[36][37][38][39][40][42][43][44][45][46]. Various classifiers used in the literature are SVM, Bayesian, Artificial Neural network, Fisher Linear Discriminator, Linear Discriminant Analysis, Bayesian etc. Feature selection techniques in Steganalysis [34][43][44][45][46][47][48][49] can effectively reduce the cost of recognition by reducing the number of features and can also provide a better classification accuracy due to finite sample size effects. Various feature selection techniques given in the literature survey are ANOVA(Analysis of Variance)[28][38][78], PSO(Particle Swarm Optimization)[47] ,Euclidean Distance[49], Principal Component Analysis[50] and respective authors have claimed that detection accuracy has improved noticeably when these techniques are applied to capture the most relevant features prior to classification. As new embedding algorithms are being designed now and then, there is still an utmost need for universal steganalysis. Dimensionality being a curse and as can be seen in literature survey features have increased from 23-D features of Fridrich[19] to 15700 given by Fengyong Li[40], hence future scope lies in universal steganalysis in fusion with feature selection.

REFERENCES

[1] N.F.Johnson, S.Jajodia, Exploring steganography: seeing the unseen, IEEE Computers, Feb 1998, Page(s):26–34.

[2] Steganography software tools, http://members.tripod.com/steganography/stego/software.html[Accessed on 12 Jan2013].

[3] A.Westfeld, F5-A steganographic algorithm: high capacity despite better steganalysis, Proceedings of Fourth International Workshop on Information Hiding, April 2001, Page(s): 289–302.

[4] W.-N. Lie and L.-C. Chang, Data hiding in images with adaptive numbers of least significant bits based on human visual system, in Proc., IEEE Int. Conf. Image Processing, 1999, Page(s): 286–290.

[5] Y. K. Lee and L. H. Chen, High capacity image steganographic model, Proc. Inst. Elect. Eng., Vis. Image Signal Processing, vol. 147, no. 3, 2000, Page(s): 288–294.

[6] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Norwood, MA: Artech House, 2000.

[7] L. M. Marvel, C. G. Boncelet Jr., and C. T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process., vol. 8, no. 8, Aug. 1999, Page(s): 1075–1083.

[8] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no. 7, Jul.1999, Page(s) 1062–1078.

[9] N.F. Johnson, S. Jajodia, Steganalysis of images created using current steganography software, in: Lecture Notes in

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

Computer Science, vol. 1525, Springer-Verlag, Berlin, pp. 273–289, 1998.

[10] R.Chandramouli, Li Grace, Nasir Memon, Adaptive steganography, in: Proc. SPIE, Security and Watermarking of Multimedia Contents IV, San Jose, CA, vol. 4675, 2002, pp. 69–78.

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

[12] A. Westfeld, A. Pfitzmann, Attacks on steganographic systems, in: Proc. of Information Hiding, Third Int. Workshop, Dresden, Germany, pp. 61–75, September 28–October 1, 1999.

[13] J. Fridrich, M. Goljan, Practical steganalysis of digital images-state of the art, in: Proc. SPIE Photonics West, Electronic Imaging (2002), Security and Watermarking of Multimedia Contents, San Jose, CA, vol. 4675, pp. 1–13, Jan 2002.

[14] R. Chandramouli, M. Kharrazi, N. Memon, Image steganography and steganalysis: Concepts and practices, in: Proc. 2nd Int. Workshop Digital Watermarking, Seoul, Korea, pp. 35–49, January 2003.

[15] J. Fridrich, R. Du, L. Meng, Steganalysis of LSB encoding in color images, in: Proc. IEEE Int. Conf. on Multimedia and Expo, New York, July 31–August 2, 2000.

[16] J. Fridrich, M. Goljan, R. Du, Detecting LSB steganography in color and gray-scale images, IEEE Multimedia Magaz., Special Issue on Security 22–28, 2001.

[17] T. Zhang, X. Ping, A fast and effective steganalytic technique against JSteg-like algorithms, in: ACM Symposium on Applied Computing, Florida, USA, March 9–12, 2003.

[18] X. Yu, Y. Wang, T. Tan, On estimation of secret message length in JSteg-like steganography, in: Proc. of 7th ICPR, 2004.

[19] J. Fridrich, Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes, in: Proc. Inf. Hiding Workshop, Lecture Notes in Computer Science, vol. 3200, Springer, pp. 67–81, 2004.

[20] Y.Shi, C.Chen, W.Chen, A Markov process based approach to effective attacking JPEG steganography, Information Hiding ,in: Proceedings of the 8th International Workshop, Springer, Berlin, 2006, pp.249–264.

[21] Dekun Zou, Yun Q. Shi, Wei Su, Guorong Xuan, Steganalysis based on Markov model of threshold prediction-error image, IEEE, ICME, 2006.

[22] Tomáˇs Pevný, Patrick Bas, and Jessica Fridrich, Steganalysis by Subtractive Pixel Adjacency Matrix, IEEE Transactions on Information Forensics and Security, Vol. 5, No. 2, pp 215- 223, June 2010.

[23] Shaohui Liu, Hongxun Yao, Wen Goa, Steganalysis of data hiding techniques in wavelet domain, in: Proc. IEEE Int. Conf. on Information Technology: Coding and Computing, 2004.

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

[25] Minh N. Do, Martin Vetterli, Wavelet-based texture retrival using generalized Gaussian density and Kullback–Leibler distance, IEEE Trans. Image Process. II pp146–158, 2002.

[26] Shaohui Liu, Hongxun Yao, Wen Goa, Steganalysis based on wavelet texture analysis and neural network, in: Proc. of WCICA 2004, Hangzhou, China, 2004.

[27] K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran, B.S. Manjunath, Steganalysis of quantization index modulation data hiding, in: Proc. ICIP, Singapore, October 2004, Page(s) 1165-1168.

[28] I. Avcibas, N. Memon, B. Sankur, Steganalysis using image quality metrics, IEEE Transactions on Image Processing, vol. 12, no. 2, pp 221-229, February 2003.

[29] H. Farid, Detecting hidden messages using higher-order statistical models, in: Proc. IEEE Int. Conf. Image Process., Rochester, NY, vol. 2, pp 905–908, September 2002.

[30] S. Lyu, H. Farid, Steganalysis using color wavelet statistics and one-class vector support machines, in: Proc. SPIE, Security, Steganography, Watermarking of Multimedia Contents, vol. 5306, 2004, Page(s): 35–45.

[31] S. Lyu, H. Farid, Steganalysis using higher order image statistics, in: IEEE Trans. Inform. Forensics and Security,vol 1, no.1 pp 111-119, 2006.

[32] Wen-Nung Lie, Guo-Shiang Lin, A feature based classification technique for blind image steganalysis, IEEE Trans. Multimedia 7 , December 2005, Page(s): 1007–1020.

[33] G. Xuan, Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions, in: Lecture Notes in Computer Science, vol. 3727, Springer-Verlag, Berlin, pp. 262–277, 2005.

[34] Y.Wang and P.Moulin ,Optimized feature extraction for learning based image steganalyis, IEEE Trans Inf Forensics Secur, vol 2, no 1, pp 262-277, 2005.

[35] Pevny, T., Fridrich, J.: Merging markov and dct features for multi-class jpeg steganalysis, IS and T/SPIE EI 2007, Lecture Notes in Computer Science, vol.6505, January 29th - February 1st 2007.

[36] Xiangyang Luo, Fenlin Liu, Shiguo Lian, Chunfang Yang, and Stefanos Gritzalis , On the Typical Statistic Features for Image Blind Steganalysis, IEEE Journal on selected areas in Communications, Vol. 29, No. 7, pp 1404-1422, August 2011.

[37] JPEG-Compatibility Steganalysis Using Block-Histogram of Recompression Artifacts, with J. Kodovský 14th Information Hiding Conference, Berkeley, CA, Springer LNCS vol. 7692, pp. 78-93, May 15–18, 2012.

[38] Shuang-Huan Zhan, Hong-Bin Zhang, Blind Steganalysis using Wavelet Statistics and ANOVA Machine Learning and Cybernetics, 2007 International Conference on Volume 5, pp:2515 – 2519,19-22 Aug. 2007.

[39] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifier for steganalysis of digital media," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 432–444, Apr. 2012.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

[40] Fengyong Li, Xinpeng Zhang, Bin Chen, and Guorui Feng, "JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier," IEEE signal processing letters, Vol. 20, No. 3, pp 233-236, March 2013.

[41] Yoan Miche, Patrick Bas, Amaury Lendasse, Christian Jutten, and Olli Simula , Advantages of Using Feature Selection Techniques on Steganalysis Schemes, Springer-Verlag Berlin Heidelberg, pp. 606-613, 2007.

[42] Q. Liu, A. H. Sung, Z. Chen, and J. Xu. Feature mining and pattern classification for steganalysis of lsb matching steganography in grayscale images. Pattern Recognition, 41(1): pp 56–66, 2008.

[43] Y. Miche, P. Bas, A. Lendasse, C. Jutten, and O. Simula, Reliable steganalysis using a minimum set of samples and features, EURASIP Journal on Information Security, doi:10.1155/2009/901381, 2009.

[44] G.K. Rajput and R.K. Agrawal, Evaluation of Feature Selection Measures for Steganalysis LNCS 5909, pp. 432–439, Springer-Verlag Berlin Heidelberg 2009.

[45] Gaurav Rajput, R.K. Agrawal, and Namita Aggarwal , Performance Evaluation of Exponential Discriminant Analysis with Feature Selection for Steganalysis, Defence Science Journal DESIDOC, Vol. 62, No. 1, pp. 19-24, January 2012.

[46] Mahdi Ramezani, Shahrokh Ghaemmaghami, Towards Genetic Feature Selection in Image Steganalysis, DOI Number: 978-1-4244-5176-0/10, IEEE, 2010

[47] Guoming Chen, Qiang Chen, Dong Zhang, Weiheng Zhu , Particle Swarm Optimization Feature Selection for Image Steganalysis, IEEE Computer Society , pp 304 – 308, 2012.

[48] Xiangyang Luo, Fenlin Liu, Jianming Chen, Yining Zhang; Image universal steganalysis based on wavelet packet transform, Multimedia Signal Processing, 2008 IEEE 10th Workshop on Digital, pp 780 - 784 2008.

[49] Ziwen Sun; Hui Li; Zhijian Wu; Zhiping Zhou, An Image Steganalysis Method Based on Characteristic Function Moments of Wavelet Subbands, Artificial Intelligence and Computational Intelligence, AICI '09. International Conference on Volume: pp 291 - 295, 2009.

[50] Li Hui, Sun Ziwen, Zhou Zhiping, An image steganalysis method based on characteristic function moments and PCA , Control Conference (CCC), 2011 30th Chinese Publication pp 3005 – 3008, 2011.

[51] Chen Dan, Chen Yuan, Wang Yu-ming, " A Universal Blind Steganalysis for Color Images", Journal of Electronic and Information Technology vol 27, 2005, Page(s) 1542-1549.

[52] T. Gireesh Kumar, R. Jithin, Shankar, Deepa, Feature Based Steganalysis Using Wavelet Decomposition and Magnitude Statistics Advances in Computer Engineering (ACE), 2010 International Conference on 2010 , Page(s): 298 - 300.

[53] Anahita Shojaei-Hashemi, Shahrokh Ghaemmaghami, Hamid Soltanian-Zadeh, and Universal Steganalysis based on Local Prediction Error in Wavelet Domain, Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011, Page(s):165-168.

[54] M.Goljan, J.Fridrich and T.Holotyak, "New Blind Steganalysis and its implications", in Proc Security, Steganography and Watermarking of Multimedia Contents VIII, SPIE vol 6072, pp 1-13, 2006.

[55] Hedieh Sajedi and Mansour Jamzad ,A Steganalysis Method Based on Contourlet Transform Coefficients , International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Page(s):245-248.

[56] Yuan-lu Tu; Sheng- rong Gong,Universal Steganalysis Using Color Correlation and Feature Fusion Information Science and Engineering, 2008. ISISE '08. International Symposium on Volume: 1, Publication Year: 2008, Page(s): 107 - 111.

[57] Zhuo Li, Kuijun Lu, Xianting Zeng, Xuezeng Pan,Feature-Based Steganalysis for JPEG Images 2009, Page(s): 76 - 80.

[58] Wenqiong Yu, Zhuo Li, Lingdi Ping, Steganalysis Algorithm Based on the D Reduction of Improved Differential Matrix in Images Pattern Recognition (CCPR), 2010 Chinese Conference on 2010 , Page(s): 1 - 7 .

[59] Spatial-frequency Feature Vector Fusion Based Steganalysis Hong Cai; Agaian, S.S.;Systems, Man and Cybernetics, 2006. SMC '06. IEEE International Conference on Volume 3, 8-11 Oct. 2006 Page(s): 1866 - 1870.

[60] Wenqiong Yu; Zhuo Li; Lingdi Ping, Blind detection for JPEG steganography Networking and Information Technology (ICNIT), 2010 International Conference on 2010 , Page(s): 128 - 132 .

[61] Deng Qian-lan, The blind detection of information hiding in color image; Computer Engineering and Technology (ICCET), 2010 2nd International Conference on Volume: 7,2010,Page(s):V7-346-V7-348.

[62] Ziwen Sun, Maomao Hui, Chao Guan, Steganalysis Based on Co-occurrence Matrix of Differential Image Intelligent Information Hiding and Multimedia Signal Processing, 2008,IIHMSP '08 International Conference on 15-17 Aug. 2008 Page(s):1097 – 1100.

[63] Jing Dong and Tieniu Tan, Blind Image Steganalysis Based on Run-Length Histogram Analysis, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, ICIP 2008, Page(s): 2064-2067.

[64] Xiaochuan Chen;Yunhong Wang; Tieniu Tan; Lei Guo; Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix Pattern Recognition, 2006. ICPR 2006, 18th International Conference on Volume 3, 0-0 0 Page(s):1107 – 1110.

[65] Shi Y.Q., Xuan G.r., Zuo D.K., Steganalysis Based on Moments of Characterstic Functions using Wavelet Decomposition, Prediction-Error Image and Neural Network, Proceedings of IEEE ICME, 2005, Page(s) 269-272.

[66] I. Avcibas, M. Kharrazib, N. Memon and B. Sankur , "Image Steganalysis with Binary Similarity Measures", EURASIP JASP, No. 17, 2005, Page(s) 2749-2757.

[67] Tomas Pevny, Jessica Fridrich, Andrew D. Ker, From Blind to Quantative Steganalysis, IEEE Transactions on

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 4, October 2013

Information Forensics and Security, Vol. 7, No. 2, 2012, Page(s) 445-454.

[68] Deng Qian-lan, Lin Jia-jun, A Universal Steganalysis Using Features Derived from the Differential Image Histogram in Frequency Domain Image and Signal Processing, 2009. CISP '09. 2nd International Congress on 2009, Page(s): 1 – 4.

[69] Jing-Qu Lin, Shang-Ping Zhong, JPEG Image Steganalysis Method Based on Binary Similarity Measures (2009), Proceedings of Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009, Page(s) 2238-2243.

[70] Shaohui Liu, Lin Ma, Hongxun Yao, Debin Zhao, Universal Steganalysis Based on Statistical Models Using Reorganization of Block-based DCT Coefficients, 2009 Fifth International Conference on Information Assurance and Security, 2009, Page(s) 778-781.

[71] Hong Zhao, Hongxia Wang, Muhammad Khurram Khan, Steganalysis for palette-based images using generalized difference image and color correlogram, Signal Processing 91 (2011) Page(s): 2595–2605.

[72] Li Zhuo, CHEN Jian, JIANG Xiao-ning," Blind JPEG Steganalysis Based on Multi-domain features, Journal of Zhejiang University (Engg Science) 2010.

[73] Wing W. Y NG, Zhi-Min He, Patrick P.K Chan, Daniel S. Yeung, Blind Steganalysis with High Generalization Capability for different Image Databases L-GEM, Proceedings of the 2011 International Conference on Machine Learning and Cybernetics, Guilin, 10-13 July, 2011, Pages 1690-1695.

[74] Shunquan Tan and Bin Li, Targeted Steganalysis of Edge adaptive Image Steganography Based on LSB Matching Revisited using B-Spline Fitting, IEEE Signal Processing Letters Vol 19, No. 6, 2012, pages 336-339.

[75] P.Sallee, Model-based steganography, in Proc. Int. Workshop on Digital Watermarking", Seoul, Korea, 2003.

[76] J. Fridrich, M. Goljan, and D. Soukal, Perturbed quantization steganography with wet paper codes, in Proc. ACM Multimedia Workshop, Germany, 2004.

[77] K. Solanki, A. Sarkar, and B.S. Manjunath, "YASS: Yet another steganographic scheme that resists blind steganalysis", 9th Int. Workshop on Info. Hiding, Saint Malo, Brittany, France, 2007.

[78] Sheikhan, M., Moin M.S., Pezhmanpour M., Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform, Intelligent Systems Design and Applications (ISDA), 2010 10th International Conference on 2010, Page(s): 368 – 372

[79] J.Kodovsky, T.Pevny and J.Fridrich, Modern steganalysis can detect YASS, Proceedings of the SPIE Electronics Imaging, Media Forensics and Security XII, San Jose:SPIE, 2010, Page(s) 1-11.

[80] Xiang Yang, Zhang Wen-hua, Effective Steganalysis of YASS Based on Statistical Moments of Wavelet Characterstic Function and Markov Process, International Conference on Computer Science and Electronics Engineering, 2012, Page(s) 606-610.

AUTHOR'S PROFILE

Ms Rita Chhikara received her B.Tech (Computers) from PREC, Pune University, M.Tech (CSE) from BMSCE, Punjab Technical University. She is currently pursuing PhD in the Department of Computer Science and Engg., ITM University, Gurgaon, Haryana, India. Presently working as Assistant Professor in Department of CSE, ITM University. Her research areas include: Data Mining and image processing. She has presented her work at both national and international forum and has 11 research publications under her name.

Dr. Latika Singh received her PhD from National Brain research centre in area of speech signal processing. Presently working as Associate Professor in Department of CSE, School of Engineering & Technology, ITM University, Gurgaon, Haryana, India. Her areas of interest mainly include signal processing. She has published 15 papers in Internal Journals of good repute. She has presented her work in several International Conferences. She has guided 10 M.Tech students, 20 B.Tech students and is presently guiding 6 PhDs.