Digital Signal Processing 20 (2010) 1758–1770

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Classification of steganalysis techniques: A study

Arooj Nissar [a], A.H. Mir [b,*]

[a] Department of Information Technology, National Institute of Technology, Srinagar 190006, India
[b] Department of Electronics and Communication, National Institute of Technology, Srinagar 190006, India

ARTICLE INFO

Article history:
Available online 13 February 2010

Keywords:
Data hiding
Steganography
Steganalysis
Signature steganalysis
Statistical steganalysis

ABSTRACT

Steganography is the art of secret communication and steganalysis is the art of detecting the hidden messages embedded in digital media using 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 statistical steganalysis have also been identified.

1. Introduction

The hostile environment, to which the electronic connection between two parties is susceptible, has led to a heightened awareness to enforce communication security in networks. The growing possibilities of innovative hostilities by adversaries have made it necessary to use new methodologies to protect data and resources from disclosure and to protect systems from network based attacks [1]. The importance of data confidentiality and data integrity has resulted in an explosive growth in the field of information hiding [2].

Cryptography [1] and steganography [3] are the two important aspects of communications security. Although cryptography is a primary method of protecting valuable information by rendering the message unintelligible to outsiders [1], steganography is a step ahead by making the communication invisible [4].

Steganography is the art of hiding the presence of communication by embedding secret messages into innocent, innocuous looking cover documents, such as digital images, videos, sound files [4]. Obviously the purpose of steganography is to avoid drawing suspicion to the transmission of hidden information. Creative techniques have been devised and used in hiding process to reduce the detectable artifacts of the embedded message. A message is hidden information in the form of plaintext, ciphertext, images or anything that can be embedded into a bit stream [5]. This message is embedded in a cover-carrier to create a stego-carrier. A possible formula of the process my be represented as

$$\text{Cover medium} + \text{Embedded message} + \text{Stegokey} = \text{Stego medium}$$

Images provide excellent carriers for hidden information and many different techniques have been introduced [6]. The common approaches for message hiding in images include LSB (Least Significant Bit) insertion methods, frequency domain techniques, spread spectrum techniques [5,6]. A survey of these techniques is given in [7]. Over the years many more techniques have emerged and accordingly digital image steganography is growing in its use and application. It may be pointed out that the concept of steganography has been misused by anti-social elements and criminals over the internet [4,8]. With the wide use and abundance of steganography tools on the internet, law enforcement authorities have concerns about the trafficking of unwanted material through web page images, audio and other files. Methods of detecting hidden

[*] Corresponding author. Fax: +91 1942420475.
E-mail addresses: chotz786@yahoo.com (A. Nissar), ajazhmir@yahoo.com (A.H. Mir).

1051-2004/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.dsp.2010.02.003

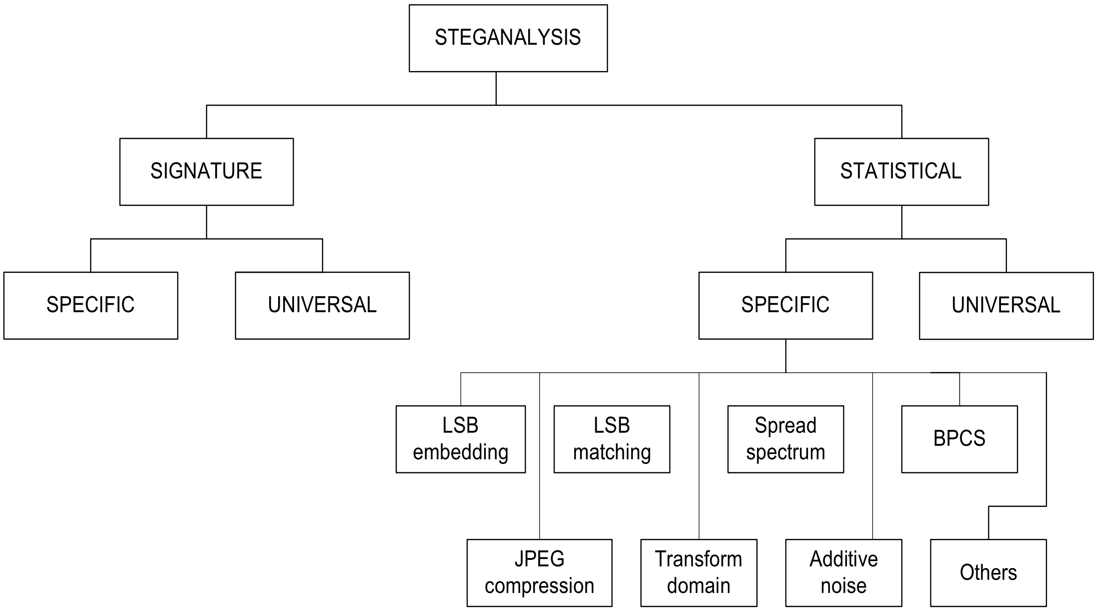

Fig. 1. The hierarchy of the classification of steganalysis techniques.

information and understanding overall structure of this technology is crucial in uncovering these activities. To achieve the objective of uncovering such activities steganalysis is being used.

Steganalysis is the art and science of detecting secret messages hidden using steganography [4,6,9]. The goal of steganalysis is to collect sufficient evidence about the presence of embedded message and to break the security of its carrier. Thus defeating the purpose of steganography. The importance of steganalytic techniques that can reliably detect the presence of hidden information in images is increasing. Steganalysis finds its use in computer forensics, cyber warfare, tracking the criminal activities over the internet and gathering evidence for investigations particularly in case of anti-social elements [4,10]. Apart from its law enforcement and anti-social significance steganalysis also has a peaceful application—improving the security of steganographic tools by evaluating and identifying their weaknesses.

With the inception of data hiding techniques the research on steganalysis started in the late 90's. Earliest work in this regard was reported by Johnson and Jajodia [6,9] and Chandramouli et al. [11]. Since then a number of different and more robust steganalysis techniques have been proposed in the literature. In this paper an attempt has been made to make a note of the various approaches proposed for the steganalysis of images and classify them. The 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 classification of steganalytic techniques is given. Section 3 deals with signature steganalysis techniques. The statistical steganalytic techniques are discussed in Section 4. Summary and conclusions drawn from the study have been given in Section 5.

2. Classification of steganalysis techniques

In this paper, we have broadly classified steganalysis into two classes: signature steganalysis and statistical steganalysis. The classification is based on whether the signature of the steganography technique or the statistics of image is used to detect the presence of hidden messages in images embedded using steganography. Under each class, the methods are further sub-divided into specific approaches and universal approaches. This sub-class is based on whether the technique targets a specific steganographic method or can target most of the steganographic techniques. The whole hierarchy of the classification is shown in Fig. 1.

3. 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 [6,9]. So one method for detecting the existence of hidden message in a suspicious image is to look for these obvious and repitative patterns-signatures of a steganography tool. In budding stages of steganalysis, signatures specific to steganographic tool were used to expose the possibility of hidden information. These specific signatures automatically exploit the tool used in embedding the messages

[6,9]. Such methods mainly look at palette tables in GIF images and anomalies caused therein by common stego tools. These attacks are especially applicable to palette images for LSB embedding in indices to the palette. Such attacks are simple, give promising results when message is embedded sequentially but are hard to automatize and their reliability is highly questionable [6,9,12].

3.1. Specific signature steganalysis

Hide and Seek [6], an image domain steganography software, creates stego-images with different properties depending upon the version applied. Both versions 4.1 and 5.0 of Hide and Seek share a common characteristic in the palette entries of stego-image. Investigating the palettes of 265 color images, or viewing the histogram, shows all the palette entries divisible by four for all bit values. This is a very unusual occurrence. Gray-scale images processed by version 4.1 and 5.0 have 256 triples as expected, but the range in sets of four triples from 0 to 252, with incremental steps of 4 (i.e., 0, 4, 8, ..., 248, 252). A key to detect this when images are viewed casually is that the "whitest" values in an image are 252 252 252. To date, this signature is unique to Hide and Seek. See [6] for examples of unique signatures of various steganography tools as applied to images.

In [13] 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. For more stego-signatures see [13].

Another specific steganalytic attack based on signature specific to BPCS (Bit Plane Complexity Segmentation)-steganography is proposed in [14]. In BPCS-steganography secret data is embedded by replacing blocks that appear noise like on bit planes. So blocks on bit planes are categorized as 'noise-like region' or an 'informative region' by means of the binary image feature called complexity. A complexity measure represents the density of the black or white pattern. Through several experiments it has been confirmed that an unusual shape, in the form of valley, in the complexity histogram is seen in stego images, formed using BPCS-steganography, than that in the original one. This 'valley' acts as a signature of BPCS-steganography and can be exploited for steganalysis.

3.2. Universal signature steganalysis

A signature steganalysis method proposed by Fridrich et al. is given in [12,15]. It has been shown that cover images stored in the JPEG format are a very poor choice for steganographic methods that work in spatial domain. This is because the quantization introduced by JPEG compression serves as a unique fingerprint that can be used for detections of very small modifications of the cover image; by inspecting the compatibility of the stego image with the JPEG format. In this technique the image under inspection is first divide into 8×8 blocks and the quantization matrix is extracted by analyzing the values of DCT coefficients in all 8×8 blocks. The quantization table is compared with standard JPEG quantization table for compatibility. If any block is incompatible the test image is a stego image. It is reported that this technique is very reliable and changes as small as flipping the LSB of one pixel can reliably be detected. Though rescaling or resampling the image may wipe out the JPEG signature.

4. Statistical steganalysis

Steganography embeds secret messages in images. The statistics of an image undergo alterations due to information hiding. 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 [16].

4.1. Specific statistical steganalysis

Specific statistical steganalysis include the statistical steganalysis techniques that target a specific steganography embedding technique or its slight variation. These types of techniques are developed by analyzing the embedding operation and determining certain image statistics that get modified as a result of the embedding process. The design of such techniques needs a detailed knowledge of embedding process. These techniques yield very accurate results when used against a target steganography technique.

In this paper specific statistical steganalysis has been further grouped on the basis of type of target steganography technique as:

4.1.1. LSB embedding steganalysis

By far the most popular and frequently used steganographic method is the Least Significant Bit embedding (LSB). It works by embedding message bits in the LSBs of sequentially or randomly selected pixels. The selection of pixels depends upon the secret stego key shared by the communicating parties. The popularity of the LSB embedding is due to its simplicity. Many steganographic softwares that use this technique are available for download on the internet [17]. The first ever statistical steganalysis was proposed by Westfeld and Pfitzmann [18]. 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 [8,12,18]. The reported results show that this method reliably detects sequentially embedded messages. Later, the method was generalized to detect randomly scattered messages [19–21].

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. [22]. 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 in [18] but cannot be applied to grayscale images.

A more sophisticated technique is presented by Fridrich et al. [4,12] for detection of LSB embedding in colour and grayscale images (RS steganalysis).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 decreased 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 [18]. However, it has been reported that the messages which require less than 0.005 bits per pixel are undetectable using RS steganalysis.

The steganalytic technique proposed by Avcibas et al. [23] is specific for LSB embedding algorithms. This technique looks at 7th and 8th bit planes of an image and calculates several binary similarity measures. The approach is based on the fact that correlation between contiguous bit planes as well as the binary texture characteristics within the bit planes is affected after a message is embedded in an image. In order to capture the effect made by embedding algorithms several features are calculated. Based on these features a steganalyser is instrumented with binary image similarity measures and multivariate regression is used to classify a given image as clean or stego.

A LSB specific steganalysis method is given by Dumitrescu et al. [24]. The technique has been inspired by work of Fridrich et al. [4] and is a generalized case of methods given in [25,26]. Here it has been investigated that the statistics of sample pairs of signal is highly sensitive to LSB embedding. The technique is based on a finite state machine whose states are selected multisets of sample pairs called trace multisets. The behavior of trace multisets under LSB embedding operations is modeled by a finite set machine. The structure of this finite state machine is used to establish quadratic equations that estimate the length of embedded messages in terms of cardinalities of trace multisets. The technique precisely measures the length of embedded message, even when the hidden message is very short relative to the size of image. This method is marginally more accurate than method given in [4] but in several cases Mean Absolute Error (MAE) becomes significant due to non-equality of cardinals and non-adaptive distribution of the joint statistics of the image. Improvements of this method are proposed in [27] where marginal and joint probabilistic distributions of the image are analysed using texture co-occurrence matrix. A variant of technique given in [24] is proposed by Lu et al. [28]. In this technique the problem is treated as one of least square estimation. It has been shown that the technique improves estimation accuracy on a set of test images. Dumitrescu et al. [29] proposes another method that utilizes higher order statistics for deriving detection equations and estimates hidden message length by measuring some signature statistical quantity (distinguishing statistics). The signature statistics is identified as a function of the hidden message length that is a function of some feature vector of the signal (with known coefficients) sensitive to the length of hidden message. A characteristic function derived from feature vector which leads to cubic polynomial equations in the hidden message length is used to detect LSB steganography. The method is reported to be robust and effective on both colour and grayscale natural images.

Gradient Energy-Flipping Rate Detection (GEFR) method is proposed by Li Zhi et al. [30]. The relation between the length of the embedded message and the gradient energy forms the basis for the detection method. In this technique the gradient energy of the cover image is calculated. After calculating gradient energy, LSB embedding with different flipping rates (as discussed in the paper) is done and the resultant gradient energy of the image after each embedding is calculated. Then the Gradient Energy curve is modeled well with straight line to estimate the message length. When embedding rate is > 0.05 bits per pixel, the technique reliably detects the presence of the secret message.

Another steganalytic technique specific to LSB steganography in grayscale images is proposed by Zhang and Ping [31]. The technique uses difference image histogram as the statistical analysis tool. The translation coefficients between difference image histograms are defined as a measure of the weak correlation between the LSB plane and the rest of the planes. These translation coefficients are used to construct a classifier to discriminate the stego images from clean ones. This algorithm can detect the existence of hidden messages embedded using sequential or random LSB replacement in images and can also estimate the amount of hidden messages exactly. This algorithm shows a better performance and computation speed than RS analysis method [4] for raw lossless compression images.

A steganalytic method for palette images known as Pairs Analysis is proposed by Fridrich et al. [32]. The approach is ideally suited to 8-bit GIF images where the message bits are embedded in LSBs of indices to an ordered palette. Pairs Analysis first splits an image into colour cuts by scanning through the image and selecting only those pixels which fall into each pair of values $(0,1)$, $(2,3)$, and so on. The colour cuts are concatenated into a single stream and homogeneity of the LSBs is measured. The homogeneity is again evaluated for the alternatives pairs of values $(255,0)$, $(1,2)$, $(3,4)$, $\ldots$. This homogeneity is proved to be a quadratic function of the secret message length and hence estimation of the unknown message length from the stego image is done. This method outperforms the Chi-square attack [18]. Also, for BMP and palette images it produces more reliable results than RS steganalysis [4]. However, the RS steganalysis performs slightly better than Pairs Analysis for grayscale images. Andrew D. Ker et al. have evaluated both Pairs and RS steganalysis algorithms in [33,34] and proposed some improvements in them. It has been demonstrated by them that the performance of both methods is highly dependent upon compression. The reliability of RS steganalysis was further increased by using different masks and Pairs Analysis was improved by excluding non adjacent pixels from the homogeneity calculation. These improved methods work well on grayscale images also.

A detection scheme for messages randomly scattered in LSBs of both colour and grayscale images is proposed by E. Lin et al. [35]. This method is based on gathering and inspecting a set of image relevant features from the pixel groups of stego image. The features are measurements of correlations and similarities between groups of pixels under flipping operations. These features change with different ratios of LSB embedding. Support vector regression [36,37] is used to distinguish between the stego images and the clean images. This approach detects the existence of hidden messages as well as their size.

A steganalyser presented by M.U. Celik et al. [38] is based on changes in rate-distortion curves due to embedding. The effectiveness of the approach against LSB and Stochastic embedding algorithms has been demonstrated with varying degree of success. The algorithm is based on the observation that the steganographic algorithms invariably disturb the underlying signal statistics and therefore change the rate-distortion characteristics of the signal. The LSB detection mechanism exploits the statistical irregularities caused by embedding and employs level-embedded compression for it. For detection of Stochastic embedding the data rates are achieved by lossy compression schemes. Distortion values at different rate points are used as image features. Each original image is modified by stochastic embedding. Mean square error, mean absolute error and weighed mean square error of both marked and unmarked images are used as distortion metrics. The image features are extracted and a Bayesian classifier is trained preceded by a KL transform. This classifier is then used to classify the clean images and stego images.

A soft computing approach to steganalysis specific to LSB is proposed by Benton and Chu [39]. For detection purpose decision trees and neural networks are used independently. Decision trees are generated by both C4.5 [40] and Linear Tree [41]. The features are extracted from images that are based on the variables for estimating the embedding probability in the RS method [4]. This approach differs from original RS method; as the goal of this method is to decide whether the image contains hidden data and not in estimating the embedding probability.

Almost all the steganalytic techniques given above are specific to LSB steganography for case $L = 1$ and cannot be extended to $L > 1$ (L is the rightmost bit of a pixel). The first method to attack LSB steganalysis for $L > 1$ is proposed by X. Yu et al. [42]. This method is based on isotropy analysis. X. Yu et al. propose another LSB steganalytic method in [43] for $L > 1$. This method is an extension of [44] from the case $L = 1$ to arbitrary $L > 1$. A weighted stego image is defined first and an estimation formula is derived. The accuracy of detection of hidden information and estimation of embedding ratio of hidden messages in images is relatively high.

A steganalysis technique based on bit plane randomness tests is proposed in [45]. Two binary sequences are obtained by scanning the seventh and eighth bit planes of the image with Hilbert scan. The randomness of these two sequences is tested individually by 14 kinds of randomness tests. The results of these tests form a vector and is used to construct a SVM classifier to distinguish stego images from the clean ones. Results show the method is effective to LSB type steganography and for images with embedding rate more than 0.05 bpp using space domain LSB steganography the accuracy of the technique is higher than techniques given in [46,47].

4.1.2. LSB matching steganalysis

LSB matching [48] is another paradigm of LSB embedding and is more difficult and hard to detect as compared to simple LSB replacement.

Andew D. Ker et al. [49] proposed a steganalysis technique for LSB matching. The technique works for grayscale images. HCF (Histogram Characteristic Function) introduced in [50] for colour images is used here for detection in grayscale images. Two novel ways of applying HCF are introduced: (a) Calibrating center of mass (COM) using a downsampled image and (b) computing adjacency histogram instead of usual histogram. In their work it was observed that the downsampling operation affects the center of mass of the HCF of stego image and this variation was used as the discriminator. These two ways produced reliable detectors for LSB matching in grayscale images. However, it has been seen that the embedded message length highly affects the results. Another scheme for steganalysis of LSB matching steganography is given by Q. Liu et al. [51]. It is based on feature extraction and pattern recognition techniques. The correlation features are extracted for colour images and in addition HCFCOM feature [50] and HOMMS [52] are also taken into consideration. Statistical pattern recognition algorithms are applied to train and classify the feature sets. Results show that this scheme is highly efficient for colour images and reasonably efficient for grayscale images.

4.1.3. Spread-spectrum steganography steganalysis

Spread-spectrum image steganography hides data in a Gaussian stego noise that is added to the cover image [53]. This type of steganography, therefore, is more robust and has a low probability of detection. Despite the difficulty of its detection many steganalysis methods have been put forth over the years.

Harmsen and Pearlman [50] present a spread-spectrum steganography steganalytic method for colour images. This method exploits the properties of center of mass of HCF where center of mass is the first order moment and HCF is the Fourier Transform of image histogram. A framework for modeling additive noise information hiding is developed which allows an analysis of the effects of data hiding on the histogram of a signal. The HCF center of mass is used as a simple metric that predictably is decreased by a class of additive noise. A simple classifier, Bayesian multivariate classifier [54], is created using the framework developed with known embedding scheme (spread-spectrum steganography). Experimental results show that the technique is reliable.

Chandramouli and Subbalakshmi [55] proposed two other steganalysis schemes specific for spread spectrum steganography. First scheme is a simple estimate and subtract type algorithm that does not exploit higher order statistics. Estimation of cover image from stego image is done by standard regression techniques like wavelet based Steins Unbiased Risk Estimator (SURE) [56]. The estimated value is subtracted from the stego image to obtain the estimate of the secret message. In the other scheme an attempt is made to blindly invert the stego function using higher order statistics. Experiments show that in comparison to simple estimation scheme exploiting higher order statistics improves performance of steganalysis.

Wang and Moulin [57] proposed steganalysis technique for block DCT based steganography. Block DCT based information embedding methods introduces distinct non-stationarities into stego image. Because of block structure of DCT embedding, pairs of neighboring pixels within an 8×8 block have different statistics from those across two 8×8 blocks. Two histograms of pixel differences are computed for which a Kolmogorov–Smirnov (KS) binary hypothesis test decides whether a given image is a stego or unmarked image.

Another specific steganalysis method is given in [58] and is applicable to images embedded with secret message using adaptive spread spectrum steganography. The method is based on: Block based scatter difference detection. The cover image is first restored using a spatial filter. Then the spread spectrum process is simulated on the test image several times and the scatter (variance) of low frequency coefficients in each DCT block is estimated. Same process is applied over the estimated cover image with its own scatter gained. Eventually the difference between two scatters is used to determine whether there is spread spectrum message in the test image or not. A region estimation algorithm has been also proposed to estimate the most likely stego regions. As reported the experimental results are very promising.

Sullivan et al. [59] proposed another spread spectrum specific steganalysis for grayscale images. A Markov random chain is used to model the correlation between pixels in an image. To compare the findings for Markov random chain a Joachim's support vector machine [60] is used as a classifier. The classifier is trained with both clean images and images embedded with spread spectrum steganography. Empirical matrices or joint probability mass functions are extracted as the feature vectors. The experiments show that the results are very near to the method given in [50].

4.1.4. BPCS-steganography steganalysis

X. Yu et al. [61] propose another method specific to BPCS-steganography (Section 3.1). This approach detects the existence of hidden messages in spatial as well as transform domain. It is observed that a statistical feature called isotropy is changed after embedding using BPCS-steganography in spatial domain. This change is used for steganalysis. The decision and detection of presence of secret message is made using hypothesis testing and Chi-square test respectively. In transform domain it is observed that the histogram of the quantized wavelet sub-band coefficients of natural images distribute symmetrically around zero. Embedding using BPCS-steganography causes change in histogram which can be used to do steganalysis. The detection is done by Chi-square test. Experimental results show that the method is an effective steganalytic method of BPCS-steganography. C. Kiml et al. [62] have proposed one more technique to detect BPCS-steganography in spatial domain. This method also uses Chi-square attack which otherwise is frequently used in LSB steganalysis.

4.1.5. JPEG-compression steganography steganalysis

The plausibility of steganographic target formats increases with the amount of data transmitted in the respective format. JPEG images are widely used over internet and therefore they are an ideal target format for steganography. JSteg [63] is probably the first steganographic tool to embed into JPEG images. Steganalytic methods [18,19] are capable of detecting sequential JSteg like embedding in most of the image formats including JPEG. Zhang and Ping [64] 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.

To prevent this attack, the algorithm F5 [65] was introduced. A steganalytic attack on F5 steganographic algorithm is presented in [66]. This attack detects the message (as well as estimates the size) hidden in JPEG images using F5 algorithm. The attack is based on estimation of cover image histogram from stego image. This is done by decompressing the stego image, cropping it four pixels in both directions to remove quantization in the frequency domain and recompressing it using stego image quantization matrix. Then the baseline histograms are obtained. The number of relative modifications introduced by embedding is determined by using least square fit by comparing the estimated histograms with those of the stego image. Experimental results show relative modifications as less as 10% of the usable DCT coefficients are reliably detected.

General principles for developing steganalytic methods that can actually estimate the secret message length to the cover image imposed during embedding are presented in [67]. The approach does not use thresholds or a training data base to infer message presence or its length but is based on identifying a macroscopic quantity 'S' that sensitively depends on the number of embedded bits 'm', estimating and deriving a functional form of $S(m)$ as a function of 'm' and deriving a parameter for S either analytically or from experiments. Then the unknown message length 'q' is calculated by solving the equation $S(q) = S_{\text{stego}}$, where S_{stego} is the value of S measured for the stego image. The quantity S is called distinguishing statistics. The detection methodology was applied to F5 and OutGuess [68] algorithms for JPEG and Estego algorithm for palette images.

X. Yu et al. [69] proposed a powerful steganalysis method specific for JSteg steganography in JPEG file format. In this technique first the statistical distribution of quantized DCT coefficients are modeled using generalized Cauchy distribution. The cover image histogram of DCT coefficients is estimated from the stego image histogram. As reported this estimation is more accurate than Fridrichs cropping method. From the results of these two histograms the detection is carried out using Chi-square test and the message length is also estimated.

Fridrich [70] 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. A Fisher Linear Discriminant classifier is trained on feature vectors corresponding to cover and stego images. F5, OutGuess, MB1 and MB2 [71] are used to get the stego images. From experiments it is observed that detectability decreases in order: OutGuess, F5, MB1, MB2. In [72], Model based JPEG steganography is reported to be cracked by using first order statistics only.

A method given in [73] specific to steganography in JPEG images describes an algorithm that uses hyper-dimensional geometric methods to model clean JPEG images. The geometric model is created using convex polytopes, hyper-spheres and hyper-ellipsoid in the attribute space. The model recognizes a JPEG stego image as anomalous when it does not match clean file model. As reported this geometric model provides superior anomaly detection.

A steganalysis method is discussed in [74] to effectively attack the advanced JPEG steganography schemes. This method use Markov empirical transition matrices to capture both intra-block and inter-block dependencies between block DCT coefficients in JPEG images. The hidden messages are sometimes independent to the cover data, and embedding process often decreases dependences existing in original cover data to some extent. Such changes are captured by second order statistics since the second order statistics considers the values of two or more observations as well as their position relative to one another in a data set. Features are extracted from empirical transition matrices by a threshold technique. These features are evaluated with SVMs [75] and then SVM is used as a classifier. The experimental results have shown that the proposed scheme outperforms the detection methods, viz., OutGuess, F5 and MBI used in modern steganography for JPEG images.

4.1.6. Transform domain steganography steganalysis

Steganalysis of images specific for wavelet domain quantization modulation technique [76] is presented by S. Liu et al. in [77]. From the histogram analysis it has been observed that histogram shape of cover image is smoother than stego image. For quantitative analysis of image features with hidden messages spectrum analysis and energy differences are used to score for differences in the histograms of clean and stego images. It has been seen that energy difference for stego images with quantization modulation method is much higher than clean images. A threshold is estimated to determine the presence or absence of hidden message. The experimental results are reported to be accurate.

A neural network based steganalysis is given in [78]. The digital images, clean as well as stego, are analysed in DFT, DCT, DWT transform domains using neural network. Neural network calculates the statistical features of images that are significantly impacted by data hiding. Neural network is trained using the statistics of the clean images and the images with hidden messages using quantization index modulation. Results indicate that the method is promising.

S. Liu et al. [79] proposed another technique specific for the detection of wavelet domain information hiding techniques. This work is based on statistical analysis of the texture of the image. In texture analysis energy distribution in frequency domain identifies texture and hence energies of wavelet sub-band are computed as texture features [80]. Wavelet coefficients in each sub-band of wavelet transform are modeled as a Generalized Gaussian Distribution (GGD) [80] with two parameters, viz., shape and scale. These parameters are good measure of image features [79] 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. This neural network is used as a discriminator to distinguish between stego and clean images.

Sullivan et al. [81] proposed a steganalysis method specific to QIM (Quantization Index Modulation) data hiding. They observed that probability mass functions of cover images with a sharp peak at the mean change considerably after QIM based data hiding. This fact is exploited for steganalysis. A standard supervised learning procedure is employed to extract feature and train the classifier. The classifier is targeted for an implementation of QIM that embeds in 8×8 blockwise DCT coefficients of an image. The results show that the scheme is very accurate.

4.1.7. Additive noise steganography steganalysis

Steganalysis methods specific to additive noise steganography, other than spread spectrum steganography, are kept in this sub-class.

The method proposed in [82] solves the problem of steganalysis in three stages. In the first stage the stego image (formed by $\pm k$ embedding steganography) is transformed into the transform domain. The histograms of the sub-band coefficients are modeled using non-stationary Generalized Gaussian Distribution [83]. The parameters of the cover image model are estimated by MAP estimator [84] to estimate the cover image. In the second stage, the stego message is estimated using MAP estimation. And in the third stage, the message length, location and sign is estimated by dividing the stego image into regions with different SNR using segmentation methods based on local variation given in [85] and extrapolating the results to the whole image. The proposed method works for both colour and grayscale images.

A steganalysis technique of binary images that are embedded by flipping pixels along boundaries is given by M. Jiang et al. [86]. This work is inspired by [4,51,67]. The proposed technique is based on the relationship between compression rate and data embedding rate. This method models steganographic embedding as an additive noise process to exploit the fact that the compressed bit rate of a given image increases when data embedding rate increases. Thus, compression rate is used as a distinguishing statistics that aids in discriminating between stego images and cover images. JBIG2 [87] binary image compression algorithm has been used to derive a quantitative relation between compression rate and data embedding rate. Same principle is applied in [88] to detect hidden information in a document image degraded by printing, photocopying etc.

M. Jiang et al. [89] proposes another steganalysis method. This method also models a steganographic system as an additive noise process to exploit the fact that mean and variance of stego signal are increasing functions of embedding rate. This distinguishing statistics is used to estimate the embedding rate without the knowledge of the cover object. A formula is also derived that directly relates with the mean and variance of stego signal. Both statistical measures are used to estimate the embedding rate.

M. Jiang et al. [90] has given steganalysis technique specific for boundary based steganography in binary documents. In boundary based steganography data is hidden along the boundaries of characters and symbols in a document by mixing small pixel disturbances amongst quantization and digitization noise. In the given steganalysis method the boundaries of characters and symbols in a document are modeled by a cubic polynomial and hence modeled as an autoregressive process. This model helps in detecting the stego images from clean ones by finding the variance of joint probability distribution of estimation error vector. Experimental results show highly accurate results.

4.1.8. Others

A technique of steganalysis for binary text images that makes use of similarity between the same characters and symbols for the purpose of detection is given in [91]. In this technique the idea of soft pattern matching used to compress binary images in JBIG2 [92] is used to pair the similar characters or symbols together for comparison. First all marks are extracted by segmentation from the whole image, then the marks are paired according to some condition and series pairs of matched marks are obtained. The embedding algorithm is assumed to be known and hence candidates for flipping are located according to the embedding algorithm. Two sets of candidate locations are formed from one pair. The randomization that occurs due to embedding affects the comparison of two instances of same character. This is exploited for steganalysis. One more technique for detection of data hiding in binary text images is given in [93]. This method also uses similarity between same characters and symbols but the embedding algorithm is not assumed to be known. This method detects the existence of a secret message hidden by the embedding algorithms which hide information by flipping Center of L-shaped patterns (COL) only.

4.2. Universal statistical steganalysis

Universal statistical steganalysis include the statistical steganalysis techniques that are not tailored for a specific steganography embedding technique. Universal statistical steganalysis is a meta-detection method in the sense that it can be adjusted, after training on clean and stego images, to detect any steganographic method; regardless of the embedding domain. The trick is to find out appropriate sensitive statistical quantities with 'distinguishing' capabilities. Neural network, clustering algorithms and other soft computing tools are then used to construct the detection model from the experimental data. These techniques do not depend on the behavior of embedding algorithms.

The first universal statistical steganalysis technique is given by Memon and co-workers in [46]. It has been 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. To identify appropriate image quality metrics, analysis of variance techniques is used. The steganalyser is build using multivariate regression on the selected image quality metrics alongwith a training set of cover and stego images. Simulation results with the chosen feature set and well known steganographic techniques indicate such an approach is able to reasonably distinguish between cover and stego images.

The universal steganalytic technique proposed by Farid presented in [94] uses a different approach for feature extraction from grayscale images. This approach uses a wavelet-like decomposition to build higher order statistical models of natural images as decompositions exhibit statistical regularities that can be exploited. The decomposition employed is based on separable quadrature mirror filters (QMFs) [95–97]. 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 [98,99] is then used to discriminate between untouched and adulterated images. In [47] a more flexible classifier, non-linear support vector machine (SVM) [100–102], is employed to afford better classification accuracy. In [103] the statistical model has been extended to first and higher order colour wavelet statistics and a one-class support vector machine (OC-SVM) [104] is employed for detection of secret messages in digital images. In [105] Farid and Lyu again extended the statistical model to include phase statistics in addition to first and higher order magnitude statistics. Here statistics are collected from colour images, yielding 432-D feature vector of magnitude and phase statistics. The experiments and results show that this method is more reliable in detecting steganography.

Harmsen and Pearlman [50] proposed a non specific detection scheme in which no explicit knowledge of the embedding method is available to construct a classifier. Only the clean images are available to train the classifier. HCFCOM is the feature used in the detection scheme. Mahalanobis-distance is used to measure the (dis)similarity of the suspicious image with the trained statistics. Mahalanobis-distance gives the statistical measure of how far a given point is from the estimated with consideration towards the variance of each variable. From experimental results it is seen that classifier performs very well with a correct classification rate of 95%.

A steganalytic technique used for halftone images presented in [106] also works without the knowledge of original cover image. Candidate halftone image are first converted into grayscale-like images by low-pass filtering. The low-pass filtered image is recursively decomposed using separable quadrature mirror filters (QMFs). A set of sub-band coefficients are generated at different scales and orientations. From these a set of statistical features namely mean, variance, kurtosis, skewness are computed. A Fisher Linear Discriminant analysis is employed to design a statistical classifier to discriminate between clean and marked images.

A steganalysis algorithm has been proposed in [107]. In this method a set of two image features are defined and utilized to determine the existence of covert channels in spatial or DCT domain. The gradient energy and the statistical variance of the Laplacian parameters form these two image features. The gradient energy characterizes the spatial domain variation of gray levels between adjacent pixels whereas the statistical variance of the Laplacian parameter measures the distributions of spectral coefficients in local macroblock areas. A non-linear neural classifier based on these two extracted features is used to achieve the purpose in a blind manner. The proposed system is effective to detect any steganography embedding technique and has been shown to give 90% positive detection rate.

A steganalysis technique based on multiple features formed by statistical moments of wavelet characteristic functions is given in [108]. The method shows that *n*th moments of wavelet of characteristic function are related to the *n*th magnitude of the derivative of the corresponding wavelet histogram and hence is sensitive to data embedding i.e., proposed features are sensitive to the changes of the histogram of wavelet sub-bands caused by embedding. 39-D feature vectors are proposed for steganalysis which include first three moments of characteristic function of wavelet sub-bands with the 3-level Haar wavelet [109] decomposition. Bayes classifier is adopted to classify the testing images. This steganalysis is effective for spread spectrum hiding methods.

In [110] a steganalysis method based on Markov Model of threshold prediction-error image is proposed. Image pixels are predicted with their neighboring pixels. The prediction error is obtained by subtracting the prediction values from the pixel value and then thresholded with a predefined threshold. The prediction-error images are modeled using Markov chain. Empirical transition matrices of Markov chain are calculated along horizontal, vertical and diagonal directions and serve as features for steganalysis. 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 in [110] that the results are effective than [47,59].

A universal steganalysis technique in which statistical moment of characteristic functions of test image, its wavelet subbands and prediction-error image are selected as feature is given in [111]. A test image is decomposed using a three-level Haar Transform [109] to get the first three moments of characteristic functions of each subband. Moreover, features from prediction-error image are also generated. A neural network is trained using these features and is used as a classifier. It has been reported that this technique outperforms the methods given in [47,50].

A blind steganalysis method in an image based on statistical analysis of empirical matrix (EM) is proposed in [112]. Features are extracted through processing of empirical matrix. The moments of projection histogram (PH) of empirical matrix and moments of characteristic function of projection histogram are extracted as features and support vector machine [60] is utilized as classifier. In addition features extracted from prediction error image [111] are included to enhance performance. Results show that this method performs better than any prior blind steganalysis method.

A steganalysis technique is presented in [113] for sequential steganography. In this technique abrupt changes in statistics due to sequential steganography are exploited to estimate the message location and length. These abrupt changes are used as a feature that distinguishes sequential steganography embedding from other types of embedding. Sequential probability ratio test is employed as a mathematical tool, and as a result cumulative sum CUSUM test statistics is derived for detecting steganography.

Texture based steganalysis for colour images is given in [114]. This method utilizes the Local Binary Pattern (LBP) texture operator [115] to examine the pixel texture patterns within neighborhood across the colour planes. LBP operator is a grayscale invariant measure that takes into account the amount of texture present in an image. Neural network is trained with general texture related statistics from clean and stego images. The outputs of LBP algorithm are provided to this artificial neural network. This results in creation of a reliable predictor of steganographic contents, even with relatively small amounts of embedded data.

5. Summary and conclusion

In the last decade many steganalytic techniques for digital media have been proposed in the literature. In this paper we have tried to make a note of various approaches used in the steganalytic methods that are applicable to digital images. The various methods have been categorized as in Fig. 1.

From the knowledge of the methods reported in this paper we infer that statistical steganalysis techniques, in any domain, are more robust and give promising results than signature steganalysis. This is because mathematical techniques are more sensitive than visual perception. Specific statistical steganalysis methods target a particular steganographic embedding algorithm. These techniques analyze the embedding operation and concentrate on some image feature or statistics which get modified by that embedding algorithm. Consequently, such steganalytic techniques specific to a steganographic embedding technique yield accurate decisions when tested only on that method and may fail if any other steganographic technique is used. A trivial change in the steganographic embedding algorithm may render specific statistical steganalysis methods useless.

Universal statistical steganalysis alleviate the deficiency of specific statistical steganalysis techniques. These methods are designed to detect messages embedded using any steganographic technique and without the knowledge of embedding technique. A classifier is trained with cover images and stego-images obtained from variety of different embedding algorithms. Classification is based on image features that are sensitive to wide variety of embedding operations. These methods are not as accurate as specific statistical steganalysis methods but are potentially capable of detecting previously unseen steganographic methods as well. These methods are flexible and can be adjusted to the changes made in the existing embedding algorithm by training the classifier once again.

Among the specific statistical methods reported in this paper the most effective methods that are specific to LSB embedding are the methods given in [29,33,35,45]. The effective methods of steganalysis that are specific to LSB matching, BPCS steganography and JPEG-compression steganography are [51,61,74] respectively. The methods given in [50,59] are effective for spread spectrum steganography and the methods given in [77,81] are effective to detect transform domain steganography. As far as universal statistical steganalysis is considered the most effective steganalysis techniques are those of given in [106,112,113,115]. The basis of the identification of most effective steganalysis techniques is the comparative study made by the authors in their papers.

In practice, since a steganalyst will not be able to know what steganographic technique is used, deploying a specific statistical steganalysis method may not be reasonable. Instead a universal statistical steganalysis method can do the job provided it successfully detects any steganographic embedding algorithm. Hence there is still an utmost need of a steganalysis technique that could detect any type of steganographic embedding algorithm with a lesser computational complexity.

References

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

[2] J. Fridrich, Applications of data hiding in digital images, in: Tutorial for the ISPACS'98 Conference in Melbourne, Australia, November 1998.

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

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

[5] N. Johnson, S. Jajodia, Exploring steganography: Seeing the unseen, IEEE Comput. 31 (2) (1998) 26–34.

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

[7] N.F. Johnson, S. Katzenbeisser, A survey of steganographic techniques, in: S. Katzenbeisser, F. Petitcolas (Eds.), Information Hiding, Artech House, Norwood, MA, 2000, pp. 43–78.

[8] T. Moerland, Steganography and Steganalysis, Leiden Institute of Advanced Computing Science, http://www.liacs.nl/home/tmoerl/privtech.pdf.

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

[10] Huaiqing Wang, Shuozhong Wang, Cyber warfare: Steganography vs. steganalysis, Commun. ACM 47 (October 2004) 76–82.

[11] 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.

[12] 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, January 2002, pp. 1–13.

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

[14] M. Niimi, R. Eason, H. Noda, E. Kawaguchi, Intensity histogram steganalysis in BPCS-steganography, in: Proc. SPIE, Security and Watermarking of Multimedia Contents III, vol. 4314, 2001, pp. 555–564.

[15] J. Fridrich, M. Goljan, R. Du, Steganalysis based on JPEG compatibility, in: SPIE Multimedia System and Applications IV, Denver, CO, August 20–24, 2001, pp. 275–280.

[16] R.A. Lerski, et al., MR image texture analysis—An approach to tissue characterization, Magn. Resonance Imaging 11 (1993) 873–887.

[17] http://home.comcast.net/~ebm.md/stego/softwarewindows.html.

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

[19] A. Westfeld, Detecting low embedding rates, in: Lecture Notes in Computer Science, vol. 2578, Springer-Verlag, Berlin, 2002, pp. 324–339.

[20] N. Provos, P. Honeyman, Detecting steganographic content on the internet, University of Michigan, Techn. Rep. CITI 01-1a, 2001.

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

[22] 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.

[23] I. Avcibas, N. Memon, B. Sankur, Image steganalysis with binary similarity measures, in: IEEE Int. Conf. on Image Processing, Rochester, New York, September 2002.

[24] S. Dumitrescu, X. Wu, Z. Wang, Detection of LSB steganography via sample pair analysis, IEEE Trans. Signal Process. (2003) 1995–2007.

[25] S. Dumitrescu, X. Wu, N. Memon, On steganalysis of random LSB embedding in continuous-tone images, in: IEEE Int. Conf. on Image Processing, Rochester, New York, September 2002.

[26] S. Dumitrescu, X. Wu, Steganalysis of LSB embedding in multimedia signals, in: IEEE ICME 2002, vol. 1, 2002, pp. 581–584.

[27] Benoit Roue, Patrick Bas, Jean-Marc Chassery, Improving LSB steganalysis using marginal and joint probabilistic distributions, in: Proc. 6th Workshop on Multimedia & Security, MM&Sec 2004, Magdeburg, Germany, September 20–21, 2004, ACM, 2004.

[28] P. Lu, X. Luo, Q. Tang, L. Shen, An improved sample pairs method for detection of LSB embedding, in: Proc. 6th Int. Workshop Inf. Hiding, Toronto, ON, Canada, May 2004.

[29] Sorina Dumitrescu, Xiaolin Wu, A new framework of LSB steganalysis of Digital Media, IEEE Trans. Signal Process. 53 (October 2005) 3936–3947.

[30] Li Zhi, Sui Ai Fen, Yang Yi Xian, A LSB steganography detection algorithm, in: Proc. IEEE Int. Symp. on Personal, Indoor and Mobile Radio Communication, 2003.

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

[32] J. Fridrich, M. Goljan, D. Soukal, Higher-order statistical steganalysis of palette images, in: Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V, Santa Clara, CA, vol. 5020, 2003, pp. 178–190.

[33] A. Ker, Quantitative evaluation of pairs and RS steganalysis, in: Proc. SPIE, Security, Steganography, Watermarking of Multimedia Contents, San Jose, CA, vol. 5306, 2004, pp. 83–97.

[34] A. Ker, Improved detection of LSB steganography in grayscale images, in: Proc. Inf. Hiding Workshop, Lecture Notes in Computer Science, vol. 3200, Springer, 2004, pp. 97–115.

[35] Erwei Lin, Edward Woertz, Moshe Kam, LSB steganalysis using support vector regression, in: Proc. IEEE, SME Information Assurance Workshop, 2003.

[36] A.J. Smola, B. Scholkopf, A tutorial on support vector regression, Techn. Rep. NC2-TR-1998 030, October 1998.

[37] N. Cristianini, J. Shawe-Taylor, An Introduction in Support Vector Machines and Other Kernel-Based Learning Methods, Cambridge University Press, 2000.

[38] M.U. Celik, G. Sharma, A.M. Tekalp, Universal image steganalysis using rate-distortion curves, in: Proc. IST/SPIE 16th Annu. Symp. Electronic Imaging Science Technology, San Jose, CA, January 2004, pp. 19–22.

[39] Ryan Benton, Henry Chu, Soft computing approach to steganalysis of LSB embedding in digital images, in: 3rd Int. Conf. on Information Technology Research and Education, 27–30 June 2005, pp. 105–109.

[40] J.R. Quinlan, C4.5: Programs for Machine Learning, Morgan Kaufmann, San Mateo, CA, 1993.

[41] J. Garna, P. Brazdil, Linear tree, Intell. Data Anal. 3 (1999) 1–22.

[42] X. Yu, T. Tan, Y. Wang, Isotropy-based detection and estimation: A general framework of LSB steganalysis, IEEE Trans. Image Process. 11 (5) (2005) 509–517.

[43] X. Yu, T. Tan, Y. Wang, Extended optimization of LSB steganalysis, in: IEEE Int. Conf. on Image Processing, vol. 2, 2005, pp. 1102–1105.

[44] J. Fridrich, M. Goljan, On estimation of secret message length in LSB steganography in spatial domain, in: Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI, San Jose, CA, vol. 5306, 2004, pp. 23–34.

[45] Xiang-dong Chen, et al., Detect LSB steganography with bit plane randomness tests, in: Proc. of 6th World Congress on Intelligent Control and Automation, China, June 21–23, 2006.

[46] I. Avcibas, N. Memon, B. Sankur, Steganalysis using image quality metrics, in: Security and Watermarking Multimedia Contents, SPIE, San Jose, CA, 2001.

[47] S. Lyu, H. Farid, Detecting hidden messages using higher-order statistics and support vector machines, in: 5th Int. Workshop on Information Hiding, Noordwijkerhout, The Netherlands, 2002.

[48] T. Sharp, An Implementation of Key-Based Digital Signal Steganography, Lecture Notes in Computer Science, vol. 2137, Springer-Verlag, New York, 2001, pp. 13–26.

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

[50] J.J. Harmsen, W.A. Pearlman, Steganalysis of additive noise modelable information hiding, in: Proc. SPIE, Electronic Imaging 2003, Security and Watermarking of Multimedia Contents, San Jose, CA, January 2003, pp. 131–142.

[51] Qingzhong Liu, Andrew H. Sung, Jianyun Xu, Bernardete M. Ribeiro, Image complexity and feature extraction for steganalysis of LSB matching steganography, in: IEEE Int. Conf. on Pattern Recognition, vol. 2, 2006, pp. 267–270.

[52] S. Lyu, H. Farid, How realistic is photorealistic, IEEE Trans. Signal Process. 53 (2) (2005) 845–850.

[53] L.M. Marvel, C.G. Boncelet Jr., C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (8) (1999) 1075–1083.

[54] R.O. Duda, P.E. Hart, H.G. Stork, Pattern Classification, second ed., Wiley–Interscience, New York, NY, 2000.

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

[56] D.L. Donoho, I.M. Johnstone, Adapting to unknown smoothness via wavelet shrinkage, J. Amer. Statist. Assoc. 90 (1995) 1200–1224.

[57] Ying Wang, Pierre Moulin, Steganalysis of block DCT image steganography, in: IEEE Workshop on Statistical Signal Processing, 2003, pp. 339–342.

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

[59] K. Sullivan, U. Madhow, S. Chandrasekaran, B.S. Manjunath, Steganalysis of spread spectrum data hiding exploiting cover memory, in: Proc. IST/SPIE 17th Annu. Symp. Electronic Imaging Science Technology, San Jose, CA, January 2005, pp. 38–46.

[60] T. Joachims, Making large-scale SVM learning practical, in: B. Scholkopf, C. Burges, A. Smola (Eds.), Advances in Kernal Methods – Support Vector Learning, MIT Press, 1999.

[61] X. Yu, T. Tan, Y. Wang, Reliable detection of BPCS-steganography in natural images, in: Proc. of ICIG, 2004.

[62] C. Kiml, S. Chul, S. Lee, W. Yang, H. Lee, Steganalysis on BPCS steganography, in: Proc. of Pacific Rim Workshop on Digital Steganography, Japan, 2003.

[63] JPEG-JSteg-V4, http://www.funet.fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz.

[64] 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.

[65] A. Westfeld, F5 – A steganographic algorithm. High capacity despite better steganalysis, in: I.S. Moskowitz (Ed.), Information Hiding, Fourth Int. Workshop, in: Lecture Notes in Computer Science, vol. 2137, Springer-Verlag, Berlin, Heidelberg, 2001, pp. 289–302.

[66] J. Fridrich, M. Goljan, D. Hogea, Steganalysis of JPEG images: Breaking the F5 algorithm, in: Proc. 5th Information Hiding Workshop, Noordwijkerhout, The Netherlands, October 2002, pp. 310–323.

[67] J. Fridrich, M. Goljan, D. Hogea, D. Soukal, Quantitative steganalysis of digital images: Estimating the secret message length, ACM Multimedia Systems J., Special Issue on Multimedia Security 9 (3) (2003) 288–302.

[68] N. Provos, OutGuess – Universal Steganography, http://www.outguess.org/, 2001.
[69] X. Yu, Y. Wang, T. Tan, On estimation of secret message length in JSteg-like steganography, in: Proc. of 7th ICPR, 2004.
[70] 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, 2004, pp. 67–81.
[71] P. Sallee, Model-based steganography, in: T. Kalker, et al. (Eds.), International Workshop on Digital Watermarking, in: Lecture Notes in Computer Science, vol. 2939, Springer, Berlin, Heidelberg, 2004, pp. 154–167.
[72] R. Bohme, A. Westfeld, Breaking Cauchy model-based JPEG steganography with first order statistics, in: ESORICS 2004, Lecture Notes in Computer Science, vol. 3193, 2004, pp. 125–140.
[73] B.T. McBride, G.L. Peterson, S.C. Gustafson, A new blind method for detecting novel steganography, Elsevier Digital Investigation 2 (2005) 50–70.
[74] Fu Dongdong, Yun Q. Shi, Dekun Zuo, Guorong Xuan, JPEG steganalysis using empirical transition matrix in block DCT domain, in: IEEE 8th Workshop on Multimedia Signal Processing, October 2006, pp. 310–313.
[75] C.C. Chang, C.J. Lin, LIBSVM: a library of support vector machines, http://www.csie.ntu.edu.tw/~cjlin/libsvm, 2001.
[76] B. Chen, G.W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, IEEE Trans. Inform. Theory 47 (4) (2001) 1423–1443.
[77] 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.
[78] Shaohui Liu, Yao Hongnun, Wen Goa, Neural network based steganalysis in still images, in: Proc. Int. Conf. on Multimedia and Expo, ICME2003, vol. 2, July 2003, pp. 509–512.
[79] Shaohui Liu, Hongxun Yao, Wen Goa, Steganalysis based on wavelet texture analysis and neural network, in: Proc. of WCICA 2004, HangZhou, China, 2004.
[80] Minh N. Do, Martin Vetterli, Wavelet-based texture retrival using generalized Gaussian density and Kullback–Leibler distance, IEEE Trans. Image Process. II (2) (2002) 146–158.
[81] K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran, B.S. Manjunath, Steganalysis of quantization index modulation data hiding, in: Proc. ICIP, Singapore, October 2004, pp. 1165–1168.
[82] T. Holotyak, J. Fridrich, D. Soukal, Stochastic approach to secret message length estimation in $\pm k$ embedding steganography, in: Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII, 2005, pp. 673–684.
[83] S.M. LoPresto, K. Ramchandran, M.T. Orchard, Image coding based on mixture modeling of wavelet coefficients and a fast estimation quantization framework, in: Proc. Data Compression Conf., March 1997.
[84] S. Voloshynovskiy, O. Koval, T. Pun, Wavelet-based denoising using non-stationary stochastic geometrical image priors, in: Proc. SPIE, Electronic Imaging, Image and Video Communications and Processing V, Santa Clara, CA, 2003.
[85] P. Felzenszwawalb, D. Huttenlocher, Image segmentation using local variation, in: Proc. IEEE Conf. on Computer Vision and Pattern Recognition, 1998, pp. 98–104.
[86] M. Jiang, X. Wu, E.K. Wong, N. Memon, Quantitative steganalysis of binary images, in: Proc. IEEE ICIP, 2004, pp. 29–32.
[87] P. Howard, F. Kossentini, et al., The emerging JBIG2 standard, IEEE Trans. Circuit Syst. Video Technol. 8 (1998) 838–848.
[88] M. Jiang, E.K. Wong, N. Memon, X. Wu, Steganalysis of degraded document images, in: IEEE 7th Workshop on Multimedia Signal Processing, October 2005, pp. 1–4.
[89] Ming Jiang, Edward Wong, Nasir Memon, Xiaolin Wu, A simple technique for estimating message lengths for additive noise steganography, in: Int. Conf. on Control, Automation, Robotics and Vision, China, December 6–9, 2004.
[90] M. Jiang, X. Wu, E.K. Wong, N. Memon, Steganalysis of boundary-based steganography using autoregressive model of digital boundaries, in: IEEE Int. Conf. on Pattern Recognition, 2004.
[91] J. Cheng, A.C. Kot, J. Liu, H. Cao, Steganalysis of data hiding in binary text images, in: Proc. of IEEE Int. Symp. on Circuits and Systems, 2005.
[92] Paul G. Howard, Text image compression using soft pattern matching, Comput. J. 40 (2–3) (1997) 146–156.
[93] J. Cheng, A.C. Kot, J. Liu, H. Cao, Steganalysis of binary text images, in: Proc. of IEEE ICASSP, IV, March 2005, pp. 689–692.
[94] H. Farid, Detecting hidden messages using higher-order statistical models, in: Proc. IEEE Int. Conf. Image Process., Rochester, NY, vol. 2, September 2002, pp. 905–908.
[95] P. Vaidyanathan, Quadrature mirror filter banks, M-band extensions and perfect reconstruction techniques, IEEE ASSP Magaz. 4 (3) (1987) 4–20.
[96] M. Vetterli, A theory of multirate filter banks, IEEE Trans. ASSP 35 (3) (1987) 356–372.
[97] E. Simoncelli, E. Adelson, Subband transforms, in: Subband Image Coding, Kluwer Academic Publishers, 1990, pp. 143–192.
[98] R. Fisher, The use of multiple measures in taxonomic problems, Ann. Eugenics 7 (1936) 179–188.
[99] R. Duda, P. Hart, Pattern Classification and Scene Analysis, John Wiley and Sons, 1973.
[100] V. Vapnik, The Nature of Statistical Learning Theory, Springer-Verlag, 1995.
[101] V. Vapnik, Statistical Learning Theory, John Wiley and Sons, 1998.
[102] C.J.C. Burges, A tutorial on support vector machines for pattern recognition, Data Mining Knowl. Discov. 2 (1998) 121–167.
[103] 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, pp. 35–45.
[104] B. Scholkopf, J. Platt, J. Shawe-Taylor, A.J. Smola, R.C. Williamson, Estimating the support of a high-dimensional distribution, Neural Computation (2001) 1443–1471.
[105] S. Lyu, H. Farid, Steganalysis using higher order image statistics, in: IEEE Trans. Inform. Forensics and Security, 2006.
[106] M. Jiang, E.K. Wong, N. Memon, X. Wu Steganalysis, of halftone images, in: IEEE ICASSP'05, vol. 2, 18–23 March 2005, pp. 793–796.
[107] Wen-Nung Lie, Guo-Shiang Lin, A feature based classification technique for blind image steganalysis, IEEE Trans. Multimedia 7 (6) (December 2005) 1007–1020.
[108] G. Xuan, et al., Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions, in: Lecture Notes in Computer Science, vol. 3727, Springer-Verlag, Berlin, 2005, pp. 262–277.
[109] Madhuri A. Joshi, Digial Image Processing: An Algorithimic Approach, Prentice Hall of India, New Delhi, 2006.
[110] Dekun Zou, Yun Q. Shi, Wei Su, Guorong Xuan, Steganalysis based on Markov model of thresholded prediction-error image, IEEE, ICME, 2006.
[111] Yun Q. Shi, et al., Image steganalysis based on moments of characteristic functions using wavelet decomposition, in: Prediction-Error Image and Neural Network, ICME, 2005, pp. 269–272.
[112] Xiaochuan Chen, Yunghong Wang, Tieniu Tan, Lei Guo, Blind image steganalysis based on statistical analysis of empirical matrix, IEEE, ICPR, 2006.
[113] S. Trivedi, R. Chandramouli, Active steganalysis of sequential steganography, in: SPIE Conf., Santa Clara, CA, 2003, pp. 123–130.
[114] Patricia Lafferty, Farid Ahmad, Texture based steganalysis: Results for color images, in: Proc. of SPIE, vol. 5561, 2004.
[115] T. Maenpaa, The local binary pattern approach to texture analysis – extensions and applications, Ph.D. dissertation, University of Oulu, 2003.

Arooj Nissar received her B.E. (2004) in Electronics and Communication from SSM College of Engineering, Kashmir. She completed her M.Tech. (Communication and Information Technology) in 2007 in Electronics and Communication from NIT, Srinagar. Presently she is working as a Lecturer in the Department of Information Technology, NIT, Srinagar. Her fields of interest are Image Processing, Steganalysis and Image forensics.

A.H. Mir received his B.E. in Electrical Engineering with specialization in Electronics and Communication from R.E.C. Srinagar. He got his M.Tech. (Computer Technology) and Ph.D. from IIT Delhi in 1989 and 1996, respectively. Presently he is working as Professor in the Department of Electronics and Communication Engineering, NIT Srinagar. His research interests are Image Processing, Information Security, Biometrics and Fuzzy Logic applications.