Chapter 1

Introduction

In this modern era of Internet and multimedia technology, exchange of information and messages among distant participants has become as easy as any other normal and usual activity in our daily life. The revolution in digital communication has made it not only very fast and reliable, but also a very effective and inexpensive operation. It is very natural that different facets of our social interaction are getting shaped differently under this revolution and one of these is the covert communication of messages through different digital media such as audio, text, images, videos etc. This brought attention of various researchers for developing and analyzing the techniques of information hiding. There exists two trends under information hiding research. Firstly, the *digital watermarking*, which is mainly used for copyright protection and authentication of digital media, has got a considerable attention of data hiding researchers from mid-90s. On the other hand, *Steganography*, which is mainly used as covert communication, has received increasing attention in this decade specifically after the unfortunate incident of 9/11, destroying World Trade Center in New York in 2001.

1.1 Information Hiding Paradigm

1.1.1 Steganography

Steganography, the word originated from Greek mythology, literally means covered writing. Basically, steganography is an art of secret communication which includes a vast array of methods of secret communication that conceal the very existence of hidden information. Traditional methods include use of invisible inks, microdots etc. Modern day steganographic techniques try to exploit the digital media images, audio files, video files etc.

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. In cryptography, everybody knows that something secret is being communicated. The challenge of a cryptanalyst is to decipher an enciphered text. On the other hand, the entire communication is kept secret in case of steganography. In any case, once the presence of hidden information is revealed or even suspected, the purpose of steganography is defeated, even if the message content is not extracted or deciphered. According to Johnson et al. [1], *"Steganography's niche in security is to supplement cryptography, not replace it. If a hidden message is encrypted, it must also be decrypted if discovered, which provides another layer of protection."*

1.1.2 Digital Watermarking and Steganography

In watermarking process, a digital signature called watermark, is embedded into a multimedia object such that the embedded signature can be detected or extracted later to authenticate about the ownership of the object. Watermark is either be visible or invisible.

There are a number of differences between steganography and watermarking including purpose, challenges and evaluation parameters. In watermarking applications like copyright protection and authentication, there is an active adversary that would attempt to remove, invalidate or forge watermarks. But, active adversary is rarely found in main stream of steganographic research. In addition, the existence of the watermark is often declared openly, and any attempt to remove or invalidate the embedded content renders the host useless. *The crucial requirement for steganography is perpetual and statistical undetectability.* Robustness of message recovery against malicious attack and signal processing is not the primary concern, as it is for watermarking. The difference between Steganography and Watermarking with respect to three relevant parameters such as payload, undetectability and robustness is depicted in Figure 1.1. They are briefly introduced below:

1. **Visual and Statistical Undetectability**: In order to avoid raising the suspicions

of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically.

2. **Size of Payload**: Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Requirements for higher payload and secure communication are often contradictory. Depending on the specific application scenarios, a trade off has to be sought.

3. **Robustness against intentional or unintentional attacks**: Robustness against intentional or unintentional signal or image processing attacks are of prime concerns in case watermarking. For steganography, robustness is considered with relatively less priority than security and payload.

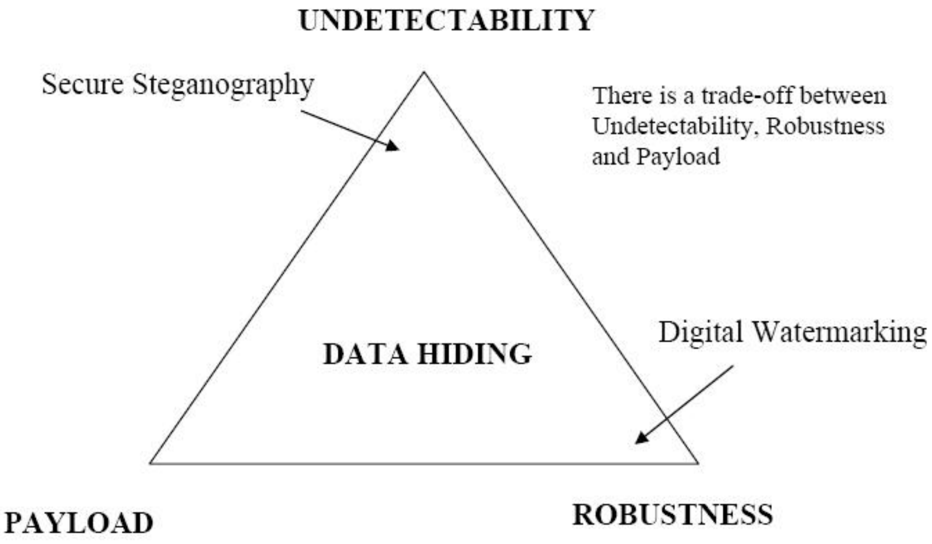

Figure 1.1: Trade off between embedding capacity, undetectability and robustness in data hiding.

1.1.3 Steganalysis

Steganalysis is the art and science of detecting messages or estimating potentially hidden information from observed data hidden by steganographic algorithms. This is analogous to cryptanalysis applied to cryptography. The goal of steganalysis is to identify suspected packages to determine whether or not they have a payload embedded, and, if possible, to recover that payload.

Steganalytic methods are roughly divided into two categories:

- Targeted Attack
- Blind Steganalysis

Targeted Attack

In a targeted attack, embedding algorithm is known to the attacker. In this case, usually statistical anomalies are considered due to embedding. A distinguishing statistics, which is the effect of the observed anomalies, is identified such that it predictively changes with length of the embedding message. Targeted attacks are more reliable than blind attacks but can not work for every different steganographic algorithm. This enforces to device a new algorithm for a new steganographic method.

Blind Steganalysis

Blind attacks, which are usually independent of steganographic algorithms, often use machine learning techniques. Firstly, suitable features are extracted from cover and stego objects. A supervised classifier is trained on the basis of these training data set to device a steganalytic detector. It is found in the literature that the feature set, extracted from the embedding domain, are most suitable for steganalytic classifier.

1.1.4 Steganographic Framework

A steganographic system may be conceived as shown in Figure 1.2. For a steganographic algorithm having a stego-key, given any cover image, the embedding process generates a stego image. The extraction process takes the stego image and using the shared key applies the inverse algorithm to extract the hidden message.

This system can be distinguished using the *'prisoners problem'* [2] (Figure 1.2) where two inmates, Alice and Bob, want to communicate in order to prepare an escape plan. The communication among them has to be secret as the warden, Wendy, examines messages passed through the public channel. Alice embeds the secret message

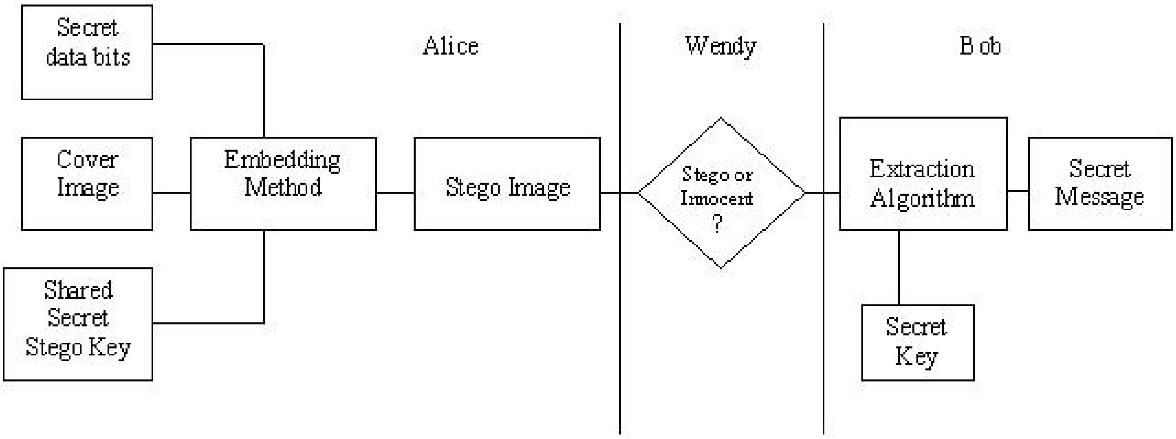

Figure 1.2: Framework for Private Key Passive Warden Steganography [3]

’m’ into the cover object ’c’, to form the stego object ’s’. In a pure steganographic framework, Wendy does not know the technique for embedding message. Only Alice and Bob know the secret. In private key steganography, they share a secret key which is used to embed the message. Though Wendy is aware of the algorithm used for embedding messages, she can not breach as she has no knowledge about the secret key. In public key steganography, Alice and Bob have private-public key pairs and know each other’s public key. In this thesis, only private key steganography is considered.

1.2 Literature Survey

In this section, a brief survey related to the work is presented. In the following subsection some of the existing steganographic techniques are briefly discussed. This is followed by discussion on some of the relevant steganalytic attacks. Out of these, a few representative methods are implemented for carrying out a comparative study, which has been discussed in the next chapter (chapter 2). It may be noted that in [3] and [4] comprehensive surveys of these techniques are reported.

1.2.1 Survey of Steganographic Algorithms

The steganographic algorithms proposed in literature can broadly be classified into two categories.

1. Spatial Domain Techniques, and
2. Transform Domain Techniques.

Spatial Domain Techniques

In spatial domain schemes, pixel gray values or color values are directly used for embedding the secret bits. These techniques are popular for their algorithmic simplicity and usual large payload.

Least Significant Bit (LSB) Replacement is the most well referred method in this category where secret bits are embedded by replacing least significant bits of the image. LSB replacement is popular for its large payload without significant visual distortion and ease of implementation. The average noise added per pixel is $0.5p$ where p is the embedding rate where the embedding rate is the number of secret bits embedded using a single pixel or coefficients (e.g. DCT coefficients) in the cover images. The usual metric for the embedding rate is bit per pixel (bpp) in case of the pixel. Sequential LSB replacement can be detected by chi-square attack [18]. As a countermeasure, secret bits are randomly scattered in the image. In spite of that LSB replacement is detected by attacks based on structural asymmetry as explained in section [1.2.2].

To overcome this undesirable asymmetry, the decision of changing the least significant bit is randomized. In this case, if the message bit does not match with the pixel bit, the pixel bit is either increased or decreased by 1. This technique is popularly known as *LSB Matching*. It is shown that even this kind of embedding adds a noise of $0.5p$ on average, where p is the embedding rate.

To further reduce the noise, the use of a binary function of two cover pixels to embed the data bits is suggested in [10]. The embedding is performed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of two pixel values carries another bit of information. It has been shown that embedding in this fashion reduces the embedding noise. In rest of the thesis, this scheme is referred as Improved LSB Matching (ILSBM).

Recently Xiaolong et al. [82] have proposed the concept of generalized LSB matching (G-LSB-M), which is an improvement over ILSBM [10]. In this paper the embedding efficiency of LSB matching scheme is improved using *sum and difference covering set (SDCS)* of finite cyclic groups. They have claimed that suitable G-LSB-M can further reduce the expected number of modification per pixel (ENMPP) and lead to more secure steganographic scheme.

The LSB replacement technique has been extended to multiple bit planes as well. Recently, it has been claimed in [5] that LSB replacement involving more than one least significant bit plane, is less detectable than the single bit plane LSB replacement against structural asymmetry based steganalysis. Hence the use of multiple bit planes for embedding has been encouraged. But the direct use of 3 or more bit planes leads to addition of considerable amount of noise in the cover image. A detailed analysis of the noise added by the LSB embedding in 3 bit planes (3LSB) is given below:

In $nLSB$ embedding, n lower significant bit planes are used for embedding. If i is the amount of noise and $P(i)$ is the corresponding probability by which i amount of noise is added to the pixel due to embedding, the expected amount of additive noise (ξ_n) during $nLSB$ is given by:

$$\xi_n = \sum_{i=1}^{2^n-1} i \times P(i) \tag{1.1}$$

Typically for n = 3, the probability of additive noise for 3LSB embedding is shown in Table 1.1. The average noise for 3LSB embedding with an embedding rate of p is computed as follows,

$\xi_3 = 1 \times \frac{7p}{32} + 2 \times \frac{3p}{16} + 3 \times \frac{5p}{32} + 4 \times \frac{p}{8} + 5 \times \frac{3p}{32} + 6 \times \frac{p}{16} + 7 \times \frac{p}{32}$

Table 1.1: The Probability of Additive Noise when Embedding is Done in Three LSBs with Embedding Rate = p

Amount	0	1	2	3	4	5	6	7
Probability	1- $\frac{7p}{8}$	$\frac{7p}{32}$	$\frac{3p}{16}$	$\frac{5p}{32}$	$\frac{p}{8}$	$\frac{3p}{32}$	$\frac{p}{16}$	$\frac{p}{32}$

= $\frac{168p}{64}$

=$2.625p \; per \; pixel.$

As 3 bits are accommodated in one pixel (since 3 least significant bit planes are used for embedding) the noise added for one bit per pixel is $2.625p/3$.

For the rest of the thesis, the notation **3LSB** is used to refer to *the LSB embedding using* 3 *least significant bit planes.*

In multiple bit plane replacement methods, multiple base notational system [6] is an interesting approach, where binary secret bit stream is converted to multiple base notational system for embedding. The amount of embedding in a pixel is controlled using this notational system depending on the local variance of that pixel. The visual quality of the stego image with respect to the the human vision sensitivity, is maintained by reducing the total perceptual error.

A similar kind of algorithm based on human vision sensitivity has been proposed in [7] by the name of Pixel Value Differencing. This approach is based on adding more data bits in the high variance regions of the image, for example, near *“the edges”* by considering the difference values of two neighboring pixels. This approach has been improved further by clubbing it with least significant bit embedding in [8].

The main drawback of multiple bit plane replacement methods is that the embedding noise is very high, which makes those schemes vulnerable against additive noise based blind attacks.

There are a few other approaches proposed in the literature. Marvel et al. [71] proposed spread spectrum image steganography (SSIS) algorithm. In this scheme, the embedded data is first modulated with pseudo random noise so that the energy is spread over a wide frequency band, achieving only a very low level of embedding strength. Thus the SSIS achieves a good level of visual imperceptibility.

Yang et al. [84] have proposed another LSB replacement technique based on adaptive embedding in the edge areas of an image. They have employed pixel value differencing, while embedding with $\pm k$ LSB replacement. More data bits are embedded in edge areas with higher k value and less bits are embedded in smooth areas of the image. It was claimed that this method achieves a large payload as well as higher image quality.

Transform Domain Techniques

In transform domain schemes, message bits are embedded using transformed coefficients of the image. Usually discrete cosine Transform (DCT), discrete wavelet transform (DWT), and integer wavelet transform (IWT) are used for these schemes.

JSteg [17] was possibly the first implementation of JPEG domain scheme where least significant bits of DCT coefficients (excluding 0 and 1 to avoid large distortion) are used for embedding sequentially. Due to the fact that JSteg introduces characteristics artifacts into the histogram of DCT coefficients, it is highly detectable using histogram based attacks [18] for sequential embedding. Even for non sequential embedding, it is detectable by other attacks [20, 72, 73].

Interestingly, preserving statistical properties of cover images is found to be one of the objectives for steganographic algorithms. Provos' Outguess algorithm [20] was an early attempt at histogram compensation for LSB hiding. First, it identifies the redundant DCT coefficients that have minimal effect on the cover image, and then depending on the information obtained in the first step, chooses bits in which it would embed the message. In other words, some of the DCT coefficients are left unchanged in the embedding process so that following the embedding, the remaining coefficients are modified to preserve the original histogram of the DCT coefficients.

Eggers et al. [46] have suggested a more rigorous approach to the same end, using histogram-preserving data-mapping (HPDM) and adaptive embedding respectively.

Another restoration based approach is Model Based Steganography, proposed by Sallee [21], where histograms of each 64 DCT coefficients in a 8×8 block are preserved.

A very recent approach in this direction is proposed by Solanki et al. in [23]. In this techniques, cover transformed coefficients are categorized into two sets. The first set is used for data embedding and the remaining set is reserved for statistical restoration. Cover statistics altered by data embedding are restored by suitably modifying the cover coefficients from the reserved set. Solanki et al. [23] have proposed a statistical restoration method where a portion of cover coefficients is allocated for embedding and another portion is used to restore the first order image statistics. To keep the Mean Square Error (MSE) at minimum while modifying the histogram, all the bins of the target histogram are compensated in an increasing order by mapping the input data with values in the same order. But it is observed that their method is not well suited for non Gaussian covers.

According to [22], *"For a given medium, the steganographic algorithm which makes fewer embedding changes or adds less additive noise, will be less detectable as compared to an algorithm which makes relatively more changes or adds higher additive noise."*. Following the same line of thought, Crandall [9] proposed to use an Error Control Coding technique called *"Matrix Encoding"*. The F5 algorithm [19] is probably the most popular implementation of Matrix Encoding. In Matrix Encoding, q message bits are embedded in a group of $2^q - 1$ cover pixels, while adding a noise of $1 - 2^{-q}$ per group on an average. The maximum embedding capacity that can be achieved by this process is $\frac{q}{2^q-1}$. For example, 2 bits of secret message are embedded in a group of 3 pixels adding a noise of 0.75 per group on average. In this case, the maximum embedding capacity achievable is $2/3$ = 0.67 bits/pixel. A detailed discussion on Matrix Encoding can be found in Crandall [9] and Westfeld [19].

Quantization Index Modulation (QIM) [58] is another important method of data hiding in transformed domain. In QIM [58], message bits are embedded into cover using quantization with a choice of quantizer indexed by the message bits. 0/1 embedding is the simple most example of QIM. Here a real valued cover sample is used for embedding a single bit. The cover sample is rounded into nearest even integer to embed a 0, while the cover sample is rounded into nearest odd integer to embed 1. The data bits are extracted by the decoder correctly if there is change in cover sample values less than 0.5 due to noise. If s is the stego signal, m is the message, and x the cover or host signal, stego signal is

$$s(x, m) = qm(x) \tag{1.2}$$

The stego signal consists only of values in the set of quantizer outputs. In the decoder, if quantized signal is not required, presence of data bits are detected due to quantized stego samples. Dither Modulation [58], can be a solution of that where quantizers are shifted using a pseudorandom sequence with a shared secret seed.

$$s(x,m) = qm(x+d) - d \tag{1.3}$$

where d is pseudorandom dither sequence.

Perturbed Quantization [22], proposed by Fridrich et al., is relatively recent approach where the sender uses the knowledge of the unquantized DCT coefficients to jointly minimize the overall distortion due to quantization and embedding. It is possible if the raw, uncompressed cover image is available to the sender rather than just its JPEG compressed form.

In the steganographic literature, it is observed that the performance of blind attack is reduced, if channel domain is separated from embedding domain. This is because calibration of channel domain macroscopic properties become useless if the embedding operation works on different domain.

Recently Solanki et al. [15] have proposed a JPEG domain steganographic algorithm called YASS based on this concept. In their scheme, embedding domain is separated from channel domain by use of randomized hiding [15]. In the YASS [15], embedding channel is used as the erasure channel. A fixed number of coefficients (typically 19 per 8×8 quantized DCT blocks) are used for embedding with a local adaptive criterion. According to the criterion, if the embedding coefficient (before or after embedding) is zero, the corresponding data bit (secret bit) is erased at the encoder. This makes the steganographic channel as an erasure channel. The resulting error has been compensated using a very powerful error control coding technique called Repeat Accumulate (RA) Coding [52]. Since number of coefficients for embedding is fixed, the number of repetition of RA code can be adjusted depending upon the amount of payload. Again the JPEG quality factor at embedding time QF_h may not be as same as the JPEG quality factor at the time of advertising the stego image QF_a. Experimentally, it is found that the resulting bit error rate (BER) is significantly high for the YASS scheme especially when the design quality (QF_h) is low. The BER increases with the increase of the design quality, but the steganalytic detectability increases as well. This is one of the most significant drawbacks of the YASS scheme. Another drawback of the YASS scheme is that it has very low embedding rate.

1.2.2 Survey of Steganalytic Attacks

The steganalytic attacks can be classified into following two groups

1. Targeted Attacks, and
2. Blind Attacks.

Targeted Attacks

In targeted attacks, corresponding steganographic algorithm is known to the attacker and the attacker tries to find out the distinguishing statistics between cover and stego images due to the given embedding algorithm. Targeted attacks often have high detection rate for the corresponding steganographic algorithm and sometimes are able to estimate the embedded message length with better accuracy. But these attacks may not always be successful against a different algorithm other than the targeted one.

An attack based on Chi-Square testing, proposed by Westfeld et al. [18] is probably the first attack made on sequential LSB replacement techniques. For a natural image (cover image), the number of odd pixels is not equal to the number of even pixels. On the other hand, at higher embedding rates these quantities tend to become equal. So, based on this artifact the ***Chi-Square Hypothesis Testing*** [18] is developed to probabilistically suggest one of the following two hypotheses:

Null Hypothesis H_0*: The given image contains stego information*
Alternative Hypothesis H_1*: The given image does not contain stego information*
The decision to accept or reject the Null Hypothesis H_0 is made on the basis of the observed confidence value p. A more detailed discussion on this analysis is made in [18].

Sample Pair Analysis, proposed by Dumitrescu et al. [34], is a targeted attack on LSB replacement where the length of an LSB embedded message in an image is analytically estimated. An important statistical identity is investigated in the scheme, which is related to certain sets of pixels in an image. This identity is very sensitive to LSB embedding, and the change in the identity quantifies the length of the embedded message.

Another attack based on similar concept of structural asymmetry called RS Steganalysis has been independently proposed by Fridrich et al. in [60]. It reliably detects even a very short message by inspecting the differences in the number of regular and singular groups for the LSB and the "shifted LSB plane".

It is found in the literature [48] that ± 1 embedding in the spatial domain induces low-pass filtering in the histogram of the image. This is true of any embedding by adding noise. Embedding makes the histogram *smoother*. Harmsen et al. has claimed in [48] that this can be quantified by computing the Centre of Mass (COM) of the Histogram Characteristic Function (HCF) (DFT of image histogram) of an image. It is observed that the COM of stego image will always be greater than that of the cover image.

This attack was further extended for LSB Matching algorithm by Ker in [39]. In this method, the COM of a cover/stego image and its calibrated version obtained by down sampling the image are computed. It has been proved empirically that

$$C(H_C) \approx C(H_{\hat{C}}) \tag{1.4}$$

$$C(H_C) - C(H_S) > C(H_{\hat{C}}) - C(H_{\hat{S}}) \tag{1.5}$$

where H_C and H_S denote cover and stego image histograms respectively. Similarly $H_{\hat{C}}\ and\ H_{\hat{S}}$ denote histogram of calibrated cover and stego images. The center of mass (COM) operation is denoted by the function C(.).

From equations (1.4) and (1.5), a dimensionless discriminator for classification is obtained as $\frac{C(H_S)}{C(H_{\hat{S}})}$. By estimating suitable threshold values of the discriminator from a set of training data, an image is classified either as cover or stego.

Another steganalytic detector, proposed by Jun Zhang et al [53], performs well especially for never compressed images. This algorithm exploits the fact that after the LSBM, local maxima of a histogram decrease and local minima increase. Consequently, the sum of the absolute differences between local extrema and their neighbors in the histogram of stego images will be smaller than that of cover images. This property is used to define a feature of discrimination in detecting the LSBM scheme.

In another targeted attack [54], the LSBM steganography using uncompressed gray scale images is considered. For a given image, another image is formed by combining the least two significant bit-planes of the given image. This new image is divided into 3×3 overlapping sub-images. According to the count of gray levels, these sub-images are grouped into four types, i.e. T_1, T_2, T_3 and T_4, where T_1 includes the sub-images in which all the pixels have the same value. Similarly T_2 contains only two different gray levels and so on. Through embedding a random sequence by LSBM and computing the alteration rate of the number of elements in T_1, it is observed that the alteration rate is usually higher in cover image than that in the corresponding stego image. This is used as the discrimination rule in this method.

Blind Attacks

Blind steganalytic attacks are independent of any steganographic algorithms. In this approach, usually a supervised classifier is trained on a set of training data. The feature set often includes the higher order statistics of cover and stego images for classification. It is found that steganalytic features extracted from the embedding domain are more sensitive to detection.

Avcibas et al. [74, 75, 76] first proposed a blind attack by introducing the concept of image quality metrics (IQMs). They conducted a statistical analysis on the sensitivity and consistent behavior of IQMs, which included mean square error, multiresolution distance measure, structural content, cross correlation, weighted spectral distance, median block weighted spectral distance, normalized absolute HVS error, mean Square HVS error, gradient measure etc. Analysis of variance (ANOVA) was also used to identify good IQMs, and the multivariate regression technique was adopted to build the classifier between cover images and stego images. It is reported that Digimarc, Coxs and PGS steganography, and Jsteg [17] steganography are reliably detected by this approach.

Farid et al. [77, 78, 79, 80] have proposed another new approach in , where higher-order probability density function (PDF) moments of subband coefficients are used as steganalytic features. An image is decomposed using separable quadrature mirror filters (QMFs). The mean, variance, skewness and kurtosis of the subband coefficients at each orientation and each scale are taken as the first set of feature vector as these statistics characterize the basic coefficient distributions. The second set of statistics is based on the errors in an optimal linear predictor of coefficients. It is from this error that additional statistics i.e. the mean, variance, skewness, and kurtosis are extracted thus forming a $24 \times (n-1)$ dimensional feature vector. For implementation purposes, n is set to 4 i.e. four level decomposition on the image is performed for extraction of features. After extraction of features, a Support Vector Machine (SVM) is used for classification. They have claimed that the Jsteg [17], and Outguess [20] algorithms are reliably detected by this method.

In similar kinds of blind attack [41, 42, 43, 44], features are extracted as statistical moments of wavelet characteristic functions. It has been claimed in [43] that *n^{th} statistical moment of a wavelet characteristic function is related to the n^{th} derivative of the corresponding wavelet histogram, and hence is sensitive to the data embedding*. A 39 dimensional feature space, which comprises of the first three moments of the characteristic functions of wavelet subbands of the three-level Haar wavelet decomposition as well as the test image, is used for the steganalysis.

In the same direction, Chen et al. [45] have proposed a steganalysis for JPEG image steganography. Steganalytic features are extracted as statistical Characterestic Function (CF) moments derived from both image pixel array and JPEG coefficient array. In this method, addition to the first-order histogram, the second-order histogram was also considered. Experimental results showed that this method outperformed the methods proposed in [6,21,36] in detecting Outguess [20], F5 [19] and Model-based steganography [21].

Wavelet Absolute Moment (WAM) steganalysis, proposed by Fridrich et al. [40], is another state of the art spatial domain blind attack, where steganalytic features are extracted from the noise residual of the stego image in wavelet domain. Wiener filter is used as the denoising filter to remove Gaussian noise from images under the assumption that the stego image is an additive mixture of a non-stationary Gaussian signal (the cover image) and a stationary Gaussian signal with a known variance (the noise) [40]. All the 27 features (statistical moments) are computed as higher order moments of the noise residual in the wavelet domain. In this technique a Fisher Linear Discriminant (FLD) is used as the classifier.

The calibration based attacks estimate the cover image statistics by nullifying the impact of embedding in the cover image. These attacks were first proposed by [14] and are designed for JPEG domain steganographic schemes. The cover image statistics is estimated by a process termed as $Self\ Calibration$. The process of self-calibration minimizes the impact of embedding in the stego image in order to estimate the cover

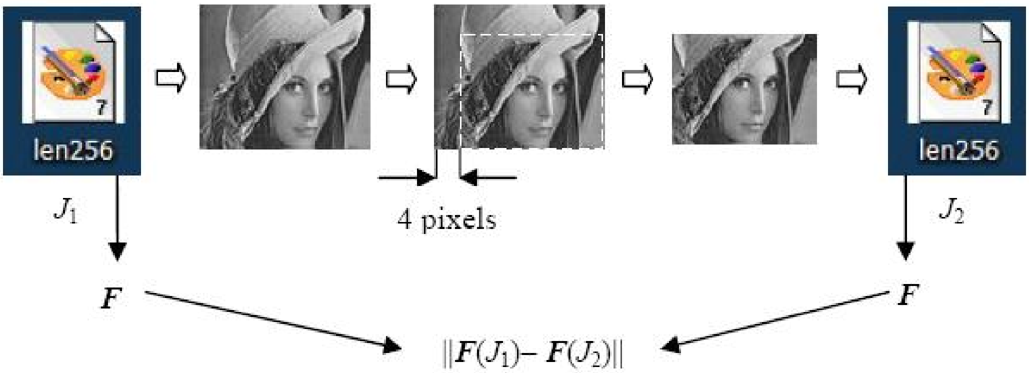

Figure 1.3: Calibration of the stego image for cover statistics estimation [14]

image features from the stego image. This calibration is done by decompressing the stego JPEG image to spatial domain and cropping 4 rows from the top and 4 columns from the left and recompressing the cropped image. The cropping and subsequent re-compression produce a "calibrated" image with most macroscopic features similar to the original cover image. The process of cropping by 4 pixels is an important step because the 8×8 grid of recompression "does not see" the previous JPEG compression and thus the obtained DCT coefficients are not influenced by previous quantization (and embedding) in the DCT domain. As in the calibration process, the quantized DCT coefficients are computed from a spatially desynchronized version of stego images, embedding impact is significantly reduced. Hence the cropping and re-compressing of a stego image helps in approximating the cover image statistics. The calibration process increases the sensitivity of the feature set to the embedding modifications while suppressing image-to-image variations. In the next two sub-sections, self-calibration based blind steganalytic attacks proposed in [14] and [29] are discussed briefly.

1. 23 Dimensional Calibration Attack

   In the 23 dimensional calibration attack [14], self calibration process is described in Figure 1.3. Let C and S be the cover and corresponding stego images and $\hat{C}$ and $\hat{S}$ be the respective cropped images. The feature set for cover images (say F_{23C}) and the stego images (say F_{23S}) are 23 dimensional vectors which are computed using the following equations

$$F_{23C}^{(i)} = \left\| g^{(i)}(C) - g^{(i)}(\hat{C}) \right\|_{L_1} \tag{1.6}$$

$$F_{23S}^{(i)} = \left\| g^{(i)}(S) - g^{(i)}(\hat{S}) \right\|_{L_1} \tag{1.7}$$

where L_1 represents the L_1 *NORM* of the two feature vectors, $i = 1, 2, \ldots 23$ and g are vector functionals which are applied to both cover and cropped cover and stego and cropped stego images. These functionals are the global DCT coefficient histogram, co-occurrence matrix, spatial blockiness measures etc. The complete set of functionals can be found in [14]. The Fisher Linear Discriminant classifier is used as steganalytic classifier. For the rest of the thesis, the notation **23DCA** is used to refer to the 23 Dimensional Calibration Attack.

2. 274 Dimensional Calibration Attack

In the 274 dimensional calibration attack, 193 extended DCT features and 81 Markov features are combined to form a 274 dimensional feature set which is then used to train the steganalytic classifier. 193 DCT features have been derived by extending the features of 23 DCA [14] and the 81 Markov features are derived from the 324 dimensional Markov features proposed in [31] which models the difference between absolute value of neighbouring DCT coefficients as a Markov process. Let C and S be the cover and corresponding stego images and $\hat{C}$ and $\hat{S}$ be the respective cropped images. The feature set for cover images (say F_{274C}) and the stego images (say F_{274S}) are 274 dimensional vectors which are computed using the following equations

$$F_{274C}(z) = \gamma_{(j)}^{(i)}(C) - \gamma_{(j)}^{(i)}(\hat{C}) \tag{1.8}$$

$$F_{274S}(z) = \gamma_{(j)}^{(i)}(S) - \gamma_{(j)}^{(i)}(\hat{S}) \tag{1.9}$$

where $z = 1, 2, \ldots 274$, $\gamma^{(i)}$ denote the vector functionals where $i = 1, 2, \ldots 21$ and $j = 1, 2, \ldots \sigma^i$ where $\sum_{i=1}^{21} \sigma^i = 274$. Each $\gamma^{(i)}$ yields σ^i features. These functionals are the global DCT coefficient histogram, co-occurrence matrix, spatial blockiness measures etc. The complete set of 21 functionals can be found in [29]. The most important difference between 23 dimensional attack and 274 dimensional attack is that in 274 dimensional attack absolute differences between cover image and cropped cover image vectors (stego image and cropped stego image vectors) are taken as cover (stego) features unlike the 23 dimensional attack where L_1 norm of the difference of the various functionals are taken as the feature set.For the rest of the thesis, the notation **274DCA** is used to refer to the 274 Dimensional Calibration Attack.

More recently, Fangjun Huang et al. [83] have proposed another JPEG domain blind attack based on microscopic and macroscopic calibration. In this method, the Markov empirical transition matrices are used to exploit not only the magnitude but also the sign dependencies existed in the intra-block and inter-block quantized DCT coefficients. Moreover, the microscopic and macroscopic calibrations are combined in the method to calibrate the local and global distribution of the quantized DCT coefficients.

Moulin [67] advocated the use of empirical PDF (probability density function) and CF (Characteristic Function) moments as features to train the classifier. Three major issues in selecting the low dimensional informative features are addressed in this technique. Firstly, a subband image representation is used for better discrimination ability than that achieved from simple wavelet transform. Two types of features, empirical moments of probability density functions (PDFs) and empirical moments of characteristic functions of the PDFs are compared. Finally, problem of feature dimensionality reduction is addressed with respect to the classification accuracy.

1.3 Motivation and Objectives

From the above survey, a few limitations of existing steganographic schemes are observed. Exploiting these limitations, different targeted and blind attacks are developed. This work is primarily motivated toward development of new algorithms to overcome these limitations and to provide better security against existing staganalytic algorithms. The specific issues in this regard are briefly discussed below:

One of the major drawbacks of embedding in multiple bit planes is that significant amount of noise is added due to this process. Against blind attacks [40], a steganographic scheme with more additive noise becomes more detectable. This fact motivates to device new techniques for reducing embedding noise in multiple bit plane steganography.

However these schemes are quite vulnerable from targeted attacks based on order statistics. As a countermeasure, one may employ statistical restoration techniques. For example, the statistical restoration technique proposed by Solanki et al. [23] is a good restoration technique in the block DCT domain. But their scheme is not well suited for images with non-Gaussian histogram. To overcome this limitation, a novel statistical restoration scheme is proposed in this work.

Once again,the limitation of the statistical restoration based steganographic method lies with the presence of extra additive noise due to restoration. This extra noise makes these schemes vulnerable against additive noise based blind attacks [40, 67]. To do away with this weakness, in this work, restoration has been carried out selectively leading to adaptive steganographic algorithms.

However, the steganographic security against blind attacks can be further enhanced by separating embedding domain from channel domain. The YASS algorithm [15] works on this principle in the block DCT domain. But its drawbacks are its very low embedding rate and high bit error rate (BER) specially when JPEG quality for embedding is relatively low (about 50%). In this thesis, new techniques on this principle have been proposed to overcome these limitations.

In brief the main objective of this work is to enhance the steganographic security against both targeted and blind attacks. This has been carried out by designing new algorithms by

1. reducing embedding noise in multiple bit plane steganography.

2. restoring statistics of cover image with a control over the addition of noise, and

3. separating embedding domain from channel domain while hiding messages.

1.4 Contribution of this Thesis

1.4.1 Reducing Embedding Noise in Multiple Bit Plane Steganography

In this work, two new steganographic algorithms are proposed to reduce the embedding noise in multiple bit plane steganography.

Method of Single Digit Sum Encoding

In this technique, a spatial domain block based encoding method is proposed, which adds less noise during embedding. Proposed block based encoding scheme combines the Single Digit Sum Encoding with Matrix Encoding to improve the steganographic security. It is analytically shown that the amount of additive noise due to embedding for the proposed scheme is less than both LSB embedding and the 3LSB scheme.

Single Digit Sum (SDS) is a $many\ to\ one$ function which is defined by the following recurrence relation:

$$T(n) = \begin{cases} n & \text{if } n < 10 \\ \\ T(\sum_{i=0}^{k-1} mod(\frac{n}{10^i}, 10)) & \text{if } n \geq 10 \end{cases} \tag{1.10}$$

where n is any k digit positive integer.

From experimental results, it is observed that the proposed scheme is relatively less detectable against Wavelet Absolute Moment Steganalyzer (WAM) [40] than the LSB embedding and the 3LSB scheme.

Multiple Bit Plane Steganography by Changing Bases

In this method, a steganographic approach has been proposed in order to reduce the embedding noise for any multiple bitplane embedding scheme. In the proposed scheme, information bit is embedded in the scaled version of a gray scale intensity value of a digital image rather than directly in it. The ability of the proposed approach to reduce noise lies on the following observation. When a small number is embedded (added or subtracted) to a higher scaled version of a number (say carrier), then the embedding distortion in the carrier is less as compared to embedding the same small number into the unscaled version of the carrier. It is experimentally shown that the total noise is reduced in the proposed scheme as compared with bare 3LSB scheme. It is also experimentally observed from the ROC plots that against the WAM based steganalyzer, the proposed scheme is less detectable than bare 3LSB embedding scheme. The proposed scheme generates more number of false positives than the 3LSB scheme.

1.4.2 Steganography Based on Statistical Restoration

In the previous work, it is observed that reduction of noise during embedding makes the corresponding steganographic algorithm more secure specially against additive noise based blind attacks. But these schemes are easily detected by some targeted attacks based on order statistics. Blind attacks also use the statistical features to train their steganalytic classifiers. As a countermeasure to these attacks, restoration of cover image statistics is another important research direction in the recent past. In this work, two statistical restoration based algorithms are devised to prevent targeted as well as blind attacks based on order statistics.

Spatial Domain Statistical Restoration

In this method, a simple statistical restoration scheme is proposed to overcome the limitation of a Gaussian cover assumption of [23] and provides better restoration of image histogram for a general cover distribution. In the proposed scheme, the image pixels are categorized into two streams, *Embedding Stream* and the *Restoration Stream*. Those pixels which are changed during embedding along with the amount of changes, are kept as meta data. Then the stego image histogram is compensated with the pixels from the *Restoration Stream* using the meta data information such that the original histogram of the cover gets restored. It is theoretically shown that the noise due to restoration process in the proposed approach is minimum, when LSB embedding is used as a steganographic method. It is experimentally shown that proposed scheme performs better than the scheme proposed by Solanki et al.[23] in restoring the image histogram for a general cover distribution.

Method of Pixel Swapping

In this technique, a pixel swapping based embedding algorithm, called *Pixel Swapping based Steganographic Algorithm ($PSSA$)*, is introduced. The proposed scheme inherently restores the image histogram and thus resists histogram based targeted attacks. The $PSSA$ is evaluated against several recent targeted steganalysis attacks which easily detect LSB matching and its improved version (ILSBM) [10]. These attacks include calibrated Histogram Characterestic Function (HCF) and HCF of Adjacency Histogram based attacks proposed by Ker [39], high frequency noise based attack by Jun Zhang et al. [53] and targeted attack by Fangjun Huang et al. [54]. It is experimentally shown that proposed $PSSA$ algorithm performs better than the $LSBM$ and the $ILSBM$ [10] schemes for most of the embedding rates.

1.4.3 Adaptive Pixel Swapping

The main drawback of the statistical restoration based steganographic method is the presence of extra additive noise due to restoration. This extra noise makes the schemes vulnerable against additive noise based blind attacks. In this work, two algorithms are proposed to improve the steganographic security of the $PSSA$ scheme by reducing the embedding noise.

Pixel Swapping based on Local Statistics

In this method, the PSSA scheme is improved by introducing a block based local adaptive threshold so that the amount of noise added (in a block) depends on certain local (within the block) image statistics. The pixel swapping is performed selectively by considering the amount of noise being added due to this process. The selection is done on the basis of local image statistics, such as, maximum, minimum and average of pixel values in that block. The algorithm is referred as the *Adaptive Pixel Swapping based Steganographic Algorithm (APSSA)*. The proposed scheme is evaluated against calibrated HCF and HCF of Adjacency Histogram based attacks proposed by Ker [39], high frequency noise based attack by Jun Zhang et al. [53] and targeted attack by Fangjun Huang et al. [54]. Experimental results reveal that at most embedding rates, proposed scheme outperforms the $LSBM$ and the $ILSBM$ schemes against mentioned targeted attacks and it is also less detectable than the $PSSA$ scheme against the

WAM steganalysis [40].

Method of Pixel Rearrangements

In this technique, another block based adaptive scheme, called *Pixel Rearrangements based Steganographic Algorithm (PRSA)*, has been introduced in order to reduce the embedding noise. In this approach, message strings (binary sequence of bits) are represented by different pixel ordering in a block. Message bits are embedded by ordering the pixels. Since embedding is done through rearrangement of pixel location, no pixel value is changed due to embedding. Thus the image histogram is inherently preserved by the scheme. It is analytically shown that the embedding noise is substantially reduces for the proposed scheme than $PSSA$ scheme. From experimental results, it is observed that proposed scheme is relatively less detectable than the $PSSA$ scheme against the WAM based blind attacks.

1.4.4 Steganography Based on Domain Separation

Reducing embedding noise by adaptive modification can improve the steganographic security to some extent against those blind attacks. To further improve the steganographic security, a new approach is considered. In this approach, the channel domain is separated from embedding domain. In this work, two such algorithms have been introduced.

Method of Spatial Desynchronization

In this method, a new steganographic scheme, called *Spatially Desynchronized Steganographic Algorithm ($SDSA$)*, based on the concept of Spatial Block Desynchronization, is proposed. A slight alteration of standard (e.g. 8x8 non overlapping block arrangement for JPEG) block arrangement can desynchronize the whole image. Such alteration of the spatial block arrangement of an image is termed as *Spatial block desynchronization*. This attempts to resist the calibration based steganalytic attacks by separating out the embedding domain from channel domain. A statistical model has been introduced to check the sensitivity of the features used in the calibration attacks and to check the effectiveness of the self-calibration process using a statistical hypothesis testing. This statistical model is used to show that the proposed $SDSA$ scheme is more robust against calibration attack than the Quantization Index Modulation (QIM) [58] and the YASS [15]. The steganographic security of $SDSA$ is evaluated against several blind steganalysis attacks and compared with performance of the YASS, which is also found to be quite robust against calibration based attacks [14, 29].

Method of Randomized Cropping

In this technique, a spatial domain steganographic scheme, called as *Steganographic Algorithm with Randomized Cropping (SARC)*, is proposed which can effectively separate the embedding domain from the channel domain using a domain randomization technique. In this approach, this domain randomization is achieved by a novel concept called *randomized cropping*. In randomized cropping, image pixels are pseudo randomly removed or cropped from the image matrix to remove (or crop) an entire row or column for separating out the embedding domain from channel domain by randomizing the spatial distribution of the image pixels. It is difficult for an attacker to design a targeted attack if proper embedding domain remains unknown. To increase the steganographic security further, embedding is done in image regions having high level of high frequency component. High frequency sub bands using wavelet decomposition are used for embedding in this approach. The choice of high frequency image regions is further tuned using on its energy content. It is experimentally found that the LSB matching encapsulated by the proposed approach greatly outperforms the simple LSB matching algorithm against the targeted attacks by Jun Zhang et al [53]. and by Fangjun Huang et al. [54] and the blind attacks by Fridrich et al. [40], and by Moulin et al. [67].

1.5 Thesis Organization

The thesis consists of seven chapters. The first chapter consists of a brief introduction of steganography paradigm, a brief literature survey, research motivation, problem statement, contribution of the thesis and the organization of the thesis.

In the second chapter the background of the research is presented. It consists of mathematical preliminaries, evaluation metrics, description of experimental dataset and performance comparisons of some representative steganographic and steganalysis schemes.

In the third chapter two algorithms have been proposed in order to reduce additive noise, where multiple bit planes are associated with embedding.

In the fourth chapter, two approaches are investigated. Firstly, a new algorithm is proposed for restoring first order statistics of the cover image after steganographic embedding in spatial domain. Secondly, a pixel swapping based steganographic method is proposed which inherently preserves the first order statistics during embedding.

In the fifth chapter, firstly, a block based pixel swapping algorithm is proposed which is an adaptive version of the Pixel Swapping scheme. Secondly, another block based algorithm is proposed where embedding noise is reduced by representing message strings using different pixel ordering of the block.

In the sixth chapter, firstly, a transformed domain algorithm is proposed where domain separation is done through spatial block desynchronization. Secondly, a spatial domain algorithm is proposed in order to enhance the security for the spatial domain schemes using the domain separation.

The seventh chapter concludes the work by summarizing the contribution of this thesis and also by suggesting future direction of research in this area.

1.6 Summary

In this chapter, motivation and objectives of this research are discussed. A brief literature survey is also provided. This is further supplemented by a comparative study in the next chapter.

Bibliography

[1] N. F. Johnson, and S. Jajodia, “Steganography: Seeing the Unseen”, *IEEE Computer*, Feb. 1998, pp. 26-34.

[2] G. Simmons, “The prisoners problem and the subliminal channel”, *Proc. of CRYPTO*, 1983, pp. 51-67.

[3] R. Chandramouli1, M. Kharrazi, N. Memon, “Image Steganography and Steganalysis:Concepts and Practice”, in *T. Kalker et al. (Eds.), Proc. of International Workshop on Digital Watermarking (IWDW 2003)*, LNCS @ Springer-Verlag Berlin Heidelberg, vol. 2939, pp. 35-49, 2004.

[4] X. Luo, D. Wang, P. Wang, F. Liu, “A review on blind detection for image steganography”, *Elsevier Journal of Signal Processing, 2008*, vol. 88, pp. 2138-2157, 2008.

[5] A. Ker,“Steganalysis of Embedding in Two Least-Significant Bits”, *IEEE Trans. on Information Forensics and Security*, vol. 2, no. 1, pp. 46-54, March 2007.

[6] X. Zhang , and S. Wang, “Steganography using multiple-base notational system and human vision sensitivity, *IEEE Signal Processing Letters*, vol. 12, Issue 1, pp. 67-70, Jan. 2005.

[7] D.C. Wu, and W.H. Tsai, “A Steganographic method for images by pixel-value differencing”, *Pattern Recognition Letters*, vol. 24, pp. 1613–1626, Jan. 2003.

[8] H.C. Wu, N.I. Wu, C.S. Tsai, and M.S. Hwang, “Image steganographic scheme based on pixel-value differencing and LSB replacement methods”, *IEE Proc. Vision, Image and Signal Processing*, vol. 152, pp. 611-615, Oct. 2005.

[9] R. Crandall, *"Some Notes on Steganography"*, Posted on Steganography Mailing List, http://os.inf.tu-dresden.de/ westfeld/crandall.pdf, 1998.

[10] J. Mielikainen,"LSB Matching Revisited", *IEEE Signal Processing Letters* , vol. 13, no. 5, pp. 285-287, May 2006.

[11] I.J. Cox, J. Kilian, F.T. Leighton, T. Shamoon, "A Secure, Robust Watermark for Multimedia", in *Proc. of the 1st Int. Workshop on Information Hiding, Cambridge, U.K*, 30th May - 1, pp. 185-206, June 1996.

[12] E. Koch, and J. Zhao, "Towards Robust and Hidden Image Copyright Labeling", in *Proc. IEEE Workshop on Nonlinear Signal and Image Processing* Halkidiki, Greece, pp. 452-455, June. 1995.

[13] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using Image Quality Metrics", *IEEE Trans. on Image Processing*, vol. 12, pp. 221-229, Feb 2003.

[14] J. Fridrich, "Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes", in *Proc. 6th Int. Workshop on Information Hiding, Toronto, Canada*, pp. 67-81, 23-25 May 2004.

[15] K. Solanki, A. Sarkar, and B.S. Manjunath, "YASS: Yet Another Steganographic Scheme that Resists Blind Steganalysis", in *Proc. 9th Int. Workshop on Information Hiding, Saint Malo, Brittany, France*, pp. 16-31, 11-13 June 2007.

[16] J. Wang , J. Li, and G. Wiederhold, "SIMPLicity : Semantics-sensitive integrated matching for picture LIbraries", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 23, no. 9, pp. 947-963, Sept. 2001.

[17] I. Avcibas, M. Kharrazi, N.D. Memon, B. Sankur., "Image steganalysis with binary similarity measures", *EURASIP Journal on Applied Signal Processing*, vol. 17, pp. 2749-2757, 2005.

[18] A. Westfeld, A. Pfitzmann, "Attacks on Steganographic Systems", in *Proc. Third International Workshop on Information Hiding, A. Pfitzmann, (ed.)*, LNCS, Springer-Verlag, Berlin Heidelberg, vol. 1768, pp. 61-76, 2000.

[19] A. Westfeld, “High capacity despite better steganalysis (F5 - a steganographic algorithm)”, in *Proc. 4th Int. Workshop on Information Hiding, Pittsburgh, PA, USA*, pp. 289-302, 25-27 April 2001.

[20] N. Provos, “Defending against statistical steganalysis”, in *Proc. 10th USENIX Security Symposium*, vol. 10, Washington DC, August 13-17, 2001.

[21] P. Sallee, “Model-based steganography”, in *Proc. 2nd International Workshop on Digital Watermarking, Seoul, Korea*, pp. 154-167, 20-20 Oct. 2003.

[22] J. Fridrich, M. Goljan, P. Lisonek, and D. Soukal, “Writing on wet paper”, *IEEE Trans. on Signal Processing*, Special Issue on Media Security, vol. 53, pp. 3923-3935, Oct. 2005.

[23] K. Solanki , K. Sullivan, U. Madhow, and B.S. Manjunath, and S. Chandrasekaran, “Statistical restoration for robust and secure steganography”, in *Proc. IEEE Int. Conf. on Image Processing, Genova, Italy*, vol. 2, pp. 1118-1121, 11-14 Sep. 2005.

[24] K. Solanki , K. Sullivan, U. Madhow, B.S. Manjunath, and S. Chandrasekaran, “Probably secure steganography: Achieving zero K-L divergence using statistical restoration”, in *Proc. IEEE Int. Conf. on Image Processing*, Atlanta, GA, USA, pp. 125-128, 8-11 Oct. 2006.

[25] K. Solanki, N. Jacobsen, U. Madhow, B.S. Manjunath, and S. Chandrasekaran, “Robust image-adaptive data hiding based on erasure and error correction”, *IEEE Trans. on Image Processing*, vol. 13, no. 12, pp. 1627-1639, Dec. 2004.

[26] M. Kharrazi, H.T. Sencar, and N. Memon, “Cover selection for steganographic embedding”, in *Proc. Int. Conf. Image Processing*, Atlanta, GA, USA, pp. 117-120, 8-11 Oct., 2006.

[27] X.G. Xia, C.G. Boncelet, and G.R. Arce, “A multiresolution watermark for digital images”, *IEEE Int. Conf. on Image Processing*, Washington, DC, USA, 26-29 Oct. 1997.

[28] S. Hetzl, and P. Mutzel, “A graph theoretic approach to steganography”, in *Proc. 9th IFIP Int. Conf. on Communications and Multimedia Security, Salzburg, Austria*, pp. 119-128, 19-21 Sep. 2005.

[29] T. Pevny , and J. Fridrich, “Merging Markov and DCT features for multi-class JPEG steganalysis”, in *Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, CA, vol. 6505 , pp. 03-04, Jan 2007.

[30] R.A. Johnson, *“Miller & Freund’s Probability and Statistics for Engineers”*, Prentice Hall of India Pvt. Ltd., New Delhi, 2003.

[31] C. Chen, Y.Q. Shi, W. Chen, and G. Xuan, “Statistical moments based universal steganalysis using JPEG-2D array and 2-D characteristic function”, in *Proc. Int. Conf. on Image Processing, Atlanta*, GA, USA, pp. 105-108, 8-11 Oct., 2006.

[32] R.O. Duda, P.E. Hart, and D.G. Stork, *“Pattern Classification”*, John Wiley & Sons Inc., New York, 2000.

[33] J. Fridrich, and D. Soukal, “Matrix Embedding for Large Payloads”, *IEEE Trans. on Information Forensics and Security*, vol. 1, pp. 390-395, Sept. 2006.

[34] S. Dumitrescu, X. Wu, and Z. Wang, “Detection of LSB steganography via sample pair analysis”,in *Proc. Information Hiding Workshop*, Springer LNCS, Vol. 2578, pp. 355 - 372, 2002.

[35] J. Fridrich, T. Pevny, and J. Kodovsky, “Statistically Undetectable JPEG Steganography: Dead Ends, Challenges, and Opportunities”, in *Proc. ACM Multimedia and Security Workshop*, Dallas, TX, pp. 3-14, 20-21 Sept. 2007.

[36] R Tzschoppe, R. Buml and J J. Eggers, *“Histogram Modifications with Minimum MSE Distortion”*, Technical Report, Erlangen, Germany, December 18, 2001.

[37] R Chandramouli , M Kharrazi and N Memon, “Image Steganography and Steganalysis: Concepts and Practices”, in *Proc. 2nd Int. Workshop on Digital Watermarking, Seoul, Korea*, pp. 35-49, 20-22 Oct. 2003.

[60] J. Fridrich, M. Goljan and R. Dui, “Reliable Detection of LSB steganography in Color and Grayscale Images”,in *Proc. ACM Workshop on Multimedia and Security*, Ottawa, CA, 5th Oct. 2001, pp. 27-30.

[39] A.D. Ker, “Steganalysis of LSB matching in grayscale images”, *IEEE Signal Processing Letters*, vol. 12, pp. 441–444, June 2005.

[40] J. Fridrich, M. Goljan, and T. Holotyak, “New Blind Steganalysis and its Implications”, in *Proc. SPIE Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072, pp. 1-13, Jan. 2006

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

[42] G.R. Xuan, J.J. Gao, Y.Q. Shi, D.K. Zou, *Image steganalysis based on statistical moments of wavelet subband histograms in DFT domain*, in: *Proceedings of IEEE International Workshop on Multimedia Signal Processing*, pp. 1-4, 2005.

[43] G.R. Xuan, Y.Q. Shi, J.J. Gao, D.K. Zou, C.Y. Yang, Z.P. Zhang, P.Q. Chai, C.H. Chen, W. Chen, “Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions”, in *Proc. of Seventh International Information Hiding Workshop*, Lecture Notes in Computer Science, Springer, Berlin, vol. 3727, pp. 262-277, 2005.

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

[45] C.H. Chen, Y.Q. Shi, W. Chen, G.R. Xuan, “Statistical moments based universal steganalysis using JPEG 2-D array and 2-D characteristic function”, in: *Proceedings of IEEE International Conference on Image Processing*, pp. 105-108, 2006.

[46] J. J. Eggers, R. Bauml, and B. Girod, “A communications approach to image

steganography", in *Proc. SPIE Security and Watermarking of Multimedia Contents IV*, vol. 4675, pp. 26-37, April 2002.

[47] J. Fridrich, M. Goljan, and D. Hogea,"Steganalysis of JPEG Images: Breaking the F5 Algorithm", in *Proc. 5th International Workshop on Information Hiding, Noordwijkerhout, The Netherlands*, pp. 310 - 323, 79 Oct. 2002.

[48] J. Harmsen, and W. Pearlman, "Steganalysis of additive noise modelable information hiding", in Proc. Security and Watermarking of Multimedia Contents V, vol. 5020, pp. 131-142, June 2003.

[49] Fridrich, J., Lisonek, P., Soukal, D.: "On Steganographic Embedding Efficiency", in *Proc. of 8th International Workshop on Information Hiding*, Alexandria, VA, LNCS, vol. 4437, pp. 282-296, 2008

[50] Zllner, J., Federrath, H., Klimant, H., Pfitzmann, A., Piotraschke, R., Westfeld, A., Wicke, G., Wolf, G., Modeling the Security of Steganographic Systems, In: Aucsmith, D. (ed.): Information Hiding. 2nd International Workshop. Lecture Notes in Computer Science, Vol. 1525. Springer-Verlag, New York, pp. 344-354, 1998.

[51] Katzenbeisser, S., Petitcolas, F. A. P.: Defining Security in Steganographic Systems, SPIE Security and Watermarking of Multimedia Contents IV, Vol. 4675, Electronic Imaging 2000, San Jose, CA, pp. 50-56, 2002.

[52] D. Divsalar, H. Jin, R. J. McEliece, "Coding theorems for turbo-like codes", in *Proc. 36 Allerton Conf. Communications, Control, Computing*, pp. 201-210, September, 1998.

[53] J. Zhang, I.J. Cox, G. Doerr, "Steganalysis for LSB Matching in Images with High-frequency Noise", *Proc. IEEE 9th Workshop on Multimedia Signal Processing, MMSP 2007*, pp. 385-388, 1-3 Oct. 2007.

[54] F. Huang, B. Li, J. Huang, "Attack LSB Matching Steganography by Counting Alteration Rate of the Number of Neighbourhood Gray Levels", *Proc. IEEE International Conference on Image Processing (ICIP 2007)*, vol. 1, pp. I401-I404, 2007.

[55] G. Schaefer, M. Stich, “UCID - An Uncompressed Colour Image Database”, *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia*, vol. 5307, pp. 472-480, 2004.

[56] A. Mayache, T. Eude, H. Cherifi, “A comparison of image quality models and metrics based on human visual sensitivity”, in *Proc . of International Conference on Image Processing, (ICIP 98)*, vol.3, pp. 409 - 413, 4-7 Oct. 1998.

[57] R. A. Horn, and C. R. Johnson, *“Norms for Vectors and Matrices”*, Chapter 5 in Matrix Analysis. Cambridge, England: Cambridge University Press, 1990.

[58] B. Chen,G. W. Wornell, “Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding”, *IEEE Transactions on Information Theory*, Volume 47, Issue 4, pp. 1423 - 1443, May 2001.

[59] A. Westfeld and A. Piftzmann, “Attacks on Steganographic Systems”, *Proc. 3rd International Workshop on Information Hiding*, Dresden, Germany, LNCS 1768, pp. 61-76, Springer-Verlag, September 29 - October 1, 1999.

[60] J. Fridrich, M. Goljan and R. Du, “Detecting LSB steganography in color and gray-scale images”, *Magazine of IEEE Multimedia Special Issue on Security*, vol. 8, no. 4, pp. 22-28, October-November 2001.

[61] A. Westfeld, “Detecting low embedding rates”, *Proc. 5th International Workshop on Information Hiding*, Noordwijkerhout, The Netherlands, LNCS, Springer-Verlag, vol. 2578, pp. 324-339, October 7-9, 2002.

[62] J. Fridrich, D. Soukal and M. Goljan, “Maximum likelihood estimation of length of secret message embedded using $\pm k$ steganography in spatial domain”, *Proc. SPIE, Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, pp. 595-606, 2005.

[63] T. Holotyak, J. Fridrich and David Soukal, “Stochastic approach to secret message length estimation in $\pm k$ embedding steganography”, *Proc. SPIE, Security, Steganography, and Watermarking of Multimedia contents VII*, vol. 5681, pp. 673-684, 2005.

[64] T. Holotyak, J. Fridrich, and S. Voloshynovskiy, "Blind statistical steganalysis of additive steganography using wavelet higher order statistics," *Proceedings of the 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security*, LNCS, vol. 3677, pp. 273–274, September 2005.

[65] S. Hetzl, and P. Mutzel, "A graph theoretic approach to steganography", in *Proc. 9th IFIP Int. Conf. on Communications and Multimedia Security, Salzburg, Austria*, pp. 119–128, 19-21 Sep. 2005.

[66] F.R. Kschischang, B.J.Frey, H. A. Loeliger, "Factor graphs and the sum-product algorithm"*IEEE Trans. on Info. Theory*, vol. 47, no. 2, pp. 498-519, 2001.

[67] Y. Wang, P. Moulin. "Optimized feature extraction for learning-based image steganalysis", *IEEE Transactions On Information Forensics and Security*, Vol. 2, No. 1, pp. 31–45, March 2007.

[68] C Cachin, "An Information Theoritic Model for Steganography", In *D. Aucsmith, editor, Proceedings of Information Hiding: Second International Workshop*, Lecture Notes in Computer Science, vol. 1525, pp. 306-318, Springer-Verlag, 1998.

[69] D. Divsalar, H. Jin, and R. J. McEliece. "Coding theorems for turbo-like codes." Proc. 36th Allerton Conf. on Communication, Control and Computing, Allerton, Illinois, pp. 201-210, Sept. 1998.

[70] H. Jin, "Analysis and Design of Turbo-Like Codes", in *Ph. D. thesis*, California Institute of Technology, Pasadena, California, pp. 20-25, May 2001.

[71] L. Marvel, C. Boncelet, C. Retter, "Spread-spectrum image steganography", *IEEE Transaction Image Process*, vol. 8, pp. 1075-1083, Aug. 1999 .

[72] X. Yu, Y. Wang, and T. Tan, "On estimation of secret message length in JSteg-like steganography", In *Proceedings, International Conference on Pattern Recognition*, Cambridge, UK, vol. 4, pp. 673-676, 23-26 August, 2004.

[73] T. Zhang and X. Ping, " A fast and effective steganalytic technique against JSteg-like algorithms", in *Proceedings of Symposium on Applied Computing*, Melbourne, FL, pp. 307-311, 2003.

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

[75] I. Avcibas, B. Sankur, K. Sayood, “Statistical evaluation of image quality measures”, *J. Electron. Imaging*, vol. 11 (2), pp. 206-223, 2002.

[76] I. Avcibas, N. Memon, B. Sankur, “Steganalysis based on image quality metrics”, in *Proceedings of the fourth IEEE Workshop on Multimedia Signal Processing*, pp. 517-522, 2001.

[77] H. Farid, “Detecting hidden messages using higher-order statistical models”, in *Proceedings of IEEE International Conference on Image processing*, vol. 2, pp. 905-908, 2002.

[78] H. Farid, S. Lyu, “Detecting hidden messages using higher-order statistics and support vector machines”, in *Proceedings of fifth International Information Hiding Workshop*, Lecture Notes in Computer Science, Springer, Berlin, vol. 2578, pp. 340-354, 2002.

[79] S. Lyu, H. Farid, “Steganalysis using color wavelet statistics and one class support vector machines”, in *Proceedings of the SPIE, Security, Steganography, and Watermarking of Multimedia Contents VI*, vol. 5306, pp. 35-45, 2004.

[80] S. Lyu, H. Farid, “Steganalysis using higher-order image statistics”, *IEEE Transaction Information Forensics Security*, vol. 1, pp. 111-119, 2006.

[81] J. Fridrich, D. Soukal, “Matrix Embedding for Large Payloads”, in *Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII*, San Jose, CA, vol. 6072, pp. W1-W15, January 16-19, 2006.

[82] X. Li, B. Yang, D. Cheng, T. Zeng, “A Generalization of LSB Matching”, in *IEEE Signal Processing Letters*, vol. 16, no. 2, pp. 69-72, February 2009.

[83] F. Huang, J. Huang, B. Li, “Universal JPEG steganalysis based on microscopic and macroscopic calibration”,in *Proc. of 15th IEEE International Conference on Image Processing (ICIP 2008)*, pp. 2068 - 2071, 12-15 Oct. 2008.

[84] C. Yang, C. Weng, S. Wang, H. Sun, “Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems”, in *IEEE Transactions on Information Forensics and Security*, vol. 3, Issue 3, pp. 488 - 497, Sept. 2008.

[85] B. Li, Y. Fang, J. Huang, “Steganalysis of Multiple-Base Notational System Steganography”,in *IEEE Signal Processing Letters*, vol. 15, pp. 493 - 496, 2008.

[86] T. Pevny, J. Fridrich, “Detection of Double-Compression in JPEG Images for Applications in Steganography”, in *IEEE Transactions on Information Forensics and Security*, vol. 3, issue 2, pp. 247 - 258, June 2008.