CHAPTER 2
STEGANOGRAPHY AND STEGANALYSIS METHODS

2.1 INTRODUCTION

The term steganography is derived from the Greek words "steganos" (covered) and "graphia" (writing). The intention of steganography is to provide the secret transmission of data. Steganalysis provides a way of detecting the presence of hidden information.

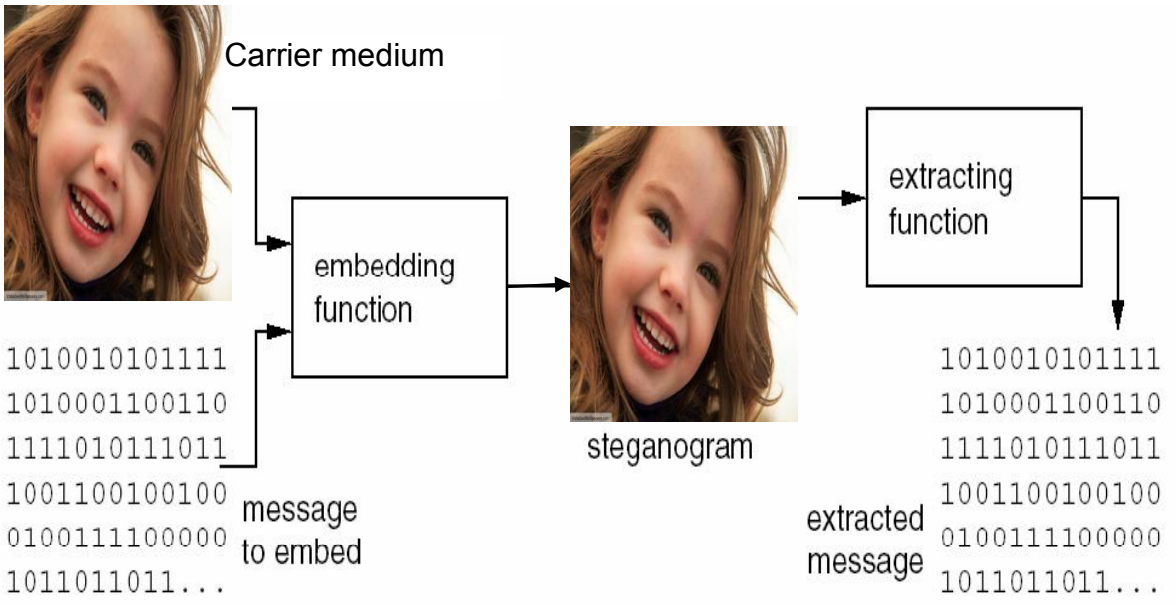

Fig. 2.1 Generic schematic view of image steganography

2.1.1 History of steganography

Steganography methods have been used for centuries. In ancient Greek times, messengers tattooed messages on their shaved heads and the messages remain invisible when their hair grows. Wax tables were used as cover source. Message to be hidden was written on the wood and was covered with new wax layer. During Second World War, milk, fruit juices, vinegar were used for writing secret messages. Invisible inks

were used to hide information in 20th century. During 1990's secret messages are hidden into some digital files. Government, industries and terrorist organization use steganography for hiding secret data.

2.1.2 Differences between steganography and cryptography

In contrast to steganography, cryptography changes the secret message from one form to another, where the message is scrambled, unreadable, and the existence of a message is often unknown. Encrypted messages can be located and intercepted but can't be decoded easily. This nature hiding information in cipher protects the message, but the interception of the message can just be as damaging because it gives clue to an opponent or enemy that someone is communicating with someone else. Steganography brings out the opposite approach and tries to hide all evidence during communication. The differences between steganography and cryptography are:

1. Steganography hides a message within another message normally called as a cover and looks like a normal graphic, video, or sound file. In cryptography, encrypted message looks like meaningless jumble of characters.
2. In steganography, a collection of graphic images, video files, or sound files in a storage medium may not leave a suspicion. In cryptography, collection of random characters on a disk will always leave a suspicion.
3. In steganography, a smart eavesdropper can detect something suspicious from a sudden change of a message format. In cryptography, smart eavesdropper can detect a secret communication from a message that has been cryptographically encoded.

4. Steganography requires caution when reusing pictures or sound files. In cryptography caution is required when reusing keys.

2.2 IMAGE STEGANOGRAPHY

Image steganography is defined as the covert embedding of data into digital pictures. Though steganography hides information in any one of the digital Medias, digital images are the most popular as carrier due to their frequency usage on the internet. Since the size of the image file is large, it can conceal large amount of information. HVS (Human Visual System) cannot differentiate the normal image and the image with hidden data. In addition with that digital images includes large amount of redundant bits, images became the most popular cover objects for steganography. Hence this research uses image as cover file.

Different image formats such as JPEG, BMP, TIFF, PNG or GIF files can be used as cover objects. A bitmap or BMP format is a simple image file format. Data is easy to manipulate, since it is uncompressed. But the uncompressed data leads to larger file size than the compressed image. JPEG (Joint Photographic Expert Group) is the most commonly used image file format. It uses lossy compression technique; the quality of the image is excellent. The size of the file is also smaller. TIFF format uses lossless compression. The file is reduced without affecting the image quality.

GIF (Graphics Interchange format) has color palette to provide an indexed colors image. It uses lossless compression. Since it can store only 256 different colors it is not suitable for representing complex photography with continuous tones, PNG (Portable Network Graphics) file format provides better colors support, best compression, and gamma correction in brightness control and image transparency. PNG format can be used as an alternative to GIF to represent web images.

2.2.1 Types of images

Digital image is represented as a set of picture element called pixel. They are organized as two dimensional arrays. Digital images can be classified according to the number of bits per pixel since the number of distinct colors of a digital image depends on number bits per pixel (bpp). There are three common types of images:

a) Binary image: In this type, one bit is allocated for each pixel. The value of a bit is represented as either 1 or 0. Each pixels of a binary image should be represented as any one of two colors (black and white). Binary image is also called as bi-level image.

b) Gray scale image: A digital image, in which the colors are represented as shades of grey, is known as grey scale image. The darkest possible shade is black, where as the highest shade is white. Each pixel is represented using eight bits. Hence, it can create 256 different shades of grey.

c) RGB or true color image: The color of each pixel is determined by the combination of red, green and blue intensities. Each pixel is represented using 24 bits, where red, green and blue components are 8 bits each. Hence, 16.7 million possible distinct colors may be represented.

2.3 CLASSIFICATION OF IMAGE STEGANOGRAPHY

The four main categories of steganography based on nature of file formats as well as the classification of image steganography are shown in Figure 2.2.

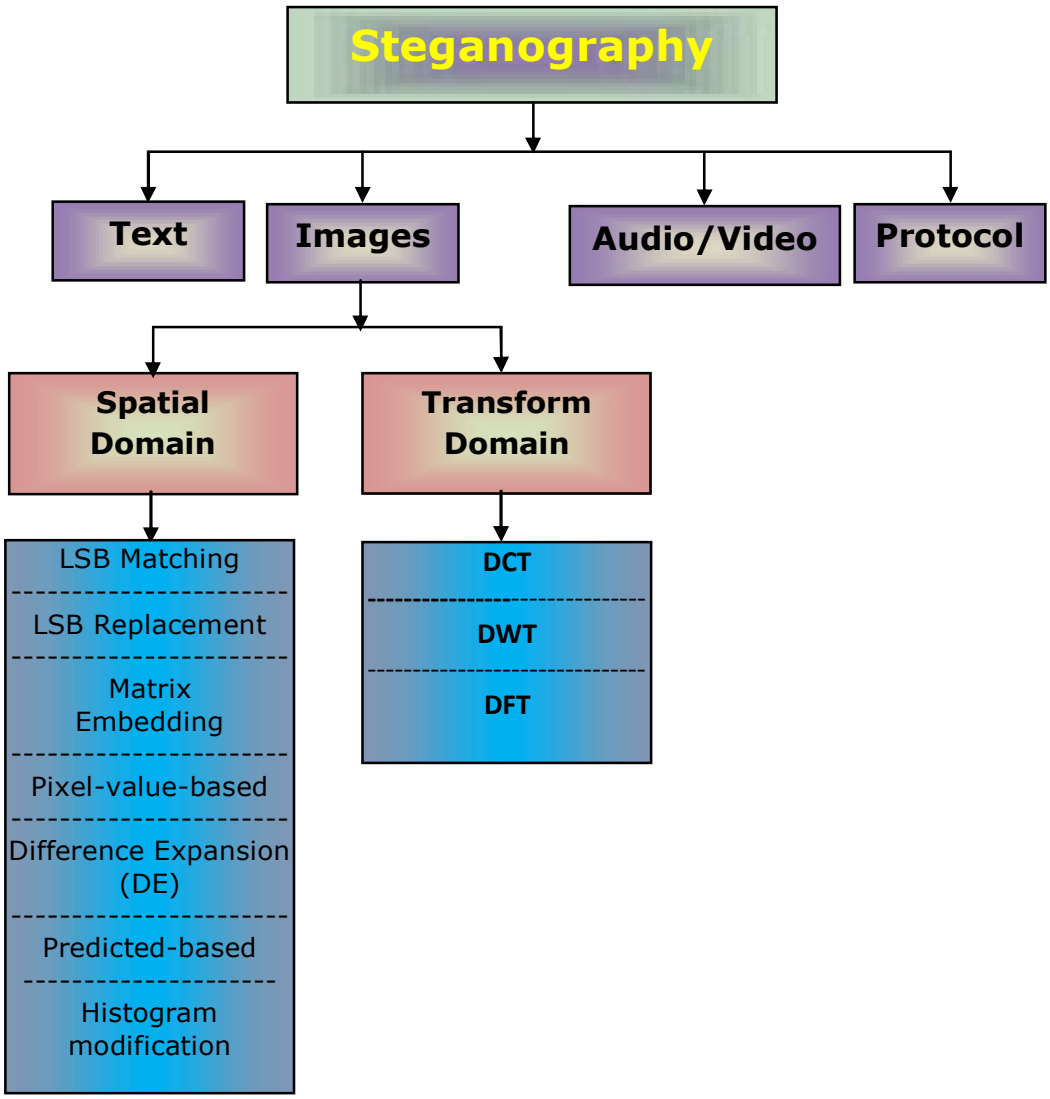

Fig. 2.2 Classification of image steganography

2.3.1 Spatial and transform domain steganography

Based on the way of embedding data into an image, image steganography techniques can be divided into the following groups:

1. Spatial domain or Image domain.
2. Transform domain or Frequency domain.

1. Spatial domain

This technique embeds messages in the intensity of the pixels directly. Some of the spatial domain methods are:

1. Least Significant Bit (LSB) Matching.
2. Least Significant Bit (LSB) Replacement.
3. Matrix Embedding.
4. Pixel-value-based image hiding.
5. Difference Expansion (DE).
6. Histogram modification.
7. Predicted based image hiding.

This research focuses on LSB Replacement method for data hiding which is described in detail in section 2.3.2. Among all message embedding techniques, the LSB insertion / modification is considered a difficult one to detect (Wayner [115]; Petitcolas et al. [83]). Spatial domain reversible data hiding is performed based on the methods difference expansion (DE) [146] and histogram modification [153], [147]. The former method provides higher capacity whereas the later provides better quality image. In DE method, the embedded bit stream includes 2 parts. The first part is the payload that conveys the secret message and the second part is the auxiliary information that contains embedding information. The size of the second part should be kept very small to increase embedding capacity.

Tian [155] proposed a prototype using DE embedding that has larger embedding capacity and also easy to embed. Ni et al. [153] proposed a reversible data hiding scheme based on histogram modification. This scheme adjusts pixel values between peak point and zero point to conceal data and to achieve reversibility. In this scheme, part of the cover image histogram is shifted rightward or leftward to produce redundancy for data embedding. Li et al. [154] proposed

reversible data hiding method called adjacent pixel difference (APD). This method is based on the neighbor pixel differences modification. In this method, an inverse 'S' order is adopted to scan the image pixels. Tai et al. [147] proposed a pixel difference based reversible data hiding scheme. Tsai et al. [156] proposed a block-based reversible data hiding scheme using prediction coding. However, this scheme had problems in prediction coding and dividing histogram into two sets.

2. Transform Domain

In Transform domain, images are first transformed and then the message is embedded into it. These are robust methods for data hiding. It is more complex method to hide secret message into an image. It performs data hiding by manipulating mathematical functions and image transformations. Transformation of cover image is performed by tweeking the coefficients and inverts the transformation. Popular transformations include the two-dimensional discrete cosine transformation (DCT) (Dongdong et al. [18]) discrete Fourier transformation (DFT) (Shi et al. [101]) and discrete wavelet transformation (DWT) (Mehrabi et al. [74]) that are commonly used in image steganalysis. The data hiding is an active field with new methods constantly introduced, thus enable as a natural way of starting the research work towards steganalysis.

2.3.2 Least Significant Bit Replacement

It is the most widely used technique for image embedding. This method became very popular due to its easy implementation. It embeds data in a cover image by replacing the least significant bits (LSB) of cover image with most significant bits (MSB) of message image which is represented in Figure 2.3.

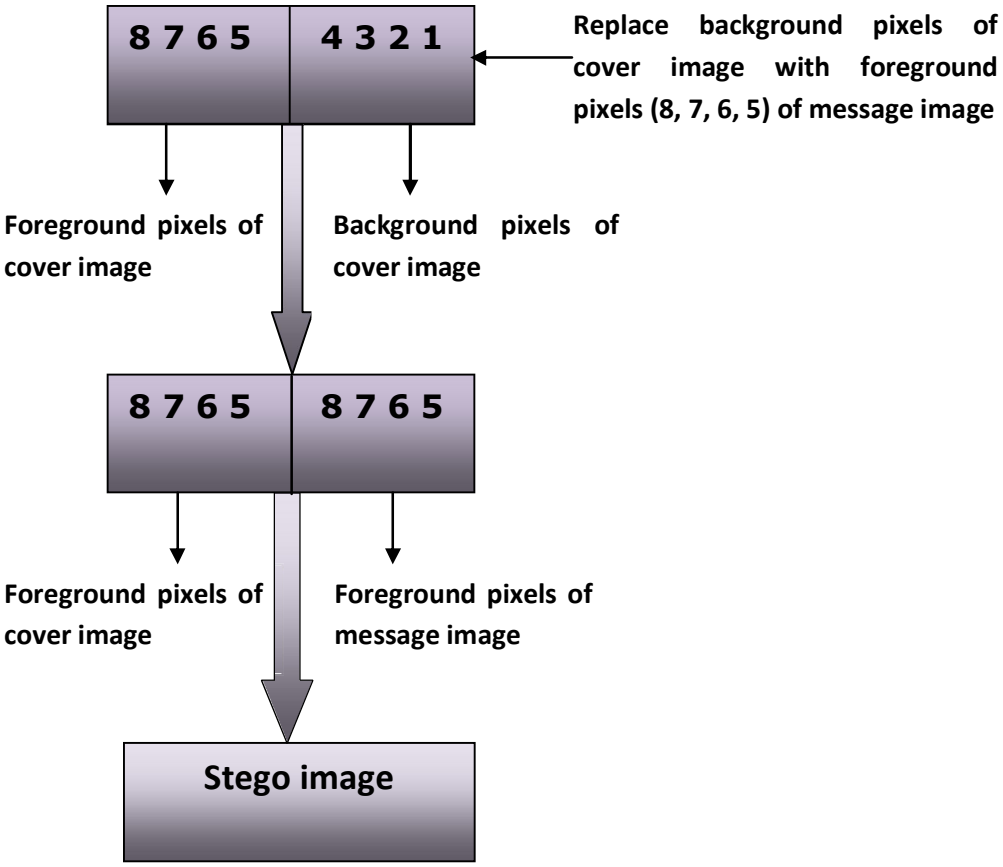

Fig. 2.3 Replacing LSB of cover image by MSB of message image

An image is represented as a collection of pixels. Each pixel is represented by 8 bits. Consider a pixel which is represented as 0110 1010. Among these 8 bits, the bits on the left side [0110] are known as MSB and the bits on the right side [1010] are known as LSB. Replacing the MSB with secret message will have noticeable impact on color. However, replacing the LSB will not be noticeable to the human eye. It produces high number of near duplicate colors. Human being can detect 6 or 7 bits of color, whereas radiologists can detect 8 or more bits of color. This method needs proper cover image to hide secret message. This method may use either 8 bit image or 24 bit image as a cover image. Each image has its own advantages and disadvantages.

When it uses 24 bit color image, large amount of space is needed to hide secret messages. It needs 24 bits (3 bytes) to represent each pixel. Among the 24 bits 3 bits (1 bit from each byte) are used to represent red, green, blue color respectively. Consider the following grid that represents the 3 pixels of a 24 bit color image.

(01101001 11010100 11010001)
(11001000 01011100 11101001)
(00100111 11001001 11101001)

From the above grid the LSB of each byte represents the red, green, blue color. Suppose we need to embed the numeric value '15' (00001111), the matrix will be modified as,

(0110100**0** 11010100 1101000**0**)
(11001000 0101110**1** 11101001)
(00100111 11001001 11101001)

The above matrix shows that it needs only **3 bits** to be modified to embed the numeric value '15' successfully. Since the resulting changes are too small, it is difficult for the human eye to recognize the changes. Hence the message is hidden successfully. But it needs large amount of space [72 bits to hide 8 bits] for embedding.

LSB may also use 8 bit image as a cover image. Even it needs smaller space to hide data, it requires a careful approach. Because it needs one byte to represent a pixel, changing the LSB of that byte will be resulting a visible changing of color. The changes will be noticeable by human eye.

Human eye cannot differentiate grey values as easy as with different colors. Gray scale images are preferred than color images. Another important aspect is the selection of compression technique. While using the lossy compression algorithm, the hidden information might be lost during decompression. Hence, it is necessary for the LSB

method to use lossless compression. The Properties of LSB embedding are:

1. LSB is a simplest method for embedding secret information into images.
2. Embedding data into least significant bit will not be perceived by the human eye. Hence the stego image looks like cover image.
3. But slight image manipulation is vulnerable for cover images.
4. Converting from GIF or BMP to JPEG and back destroy the hidden information in LSB.
5. Statistical analysis with the stego images leads to the suspicion about the hidden data.
6. As 'N' (Number of bits to be replaced) increases, hiding capacity increases but the appearance of the image degrades.

Though LSB is simplest and easiest method for embedding data into images, when more number of information is hidden, the appearance of image degrades. Statistical analysis of the stego image leads to the suspicion of hidden information.

2.4 STEGANOGRAPHIC TOOLS

Apart from the spatial domain, transform domain method for embedding secret information, various commercial soft ware's are available in the market. Some of the steganographic tools are:

1. OutGuess.
2. StegHide.
3. JPHS.
4. JSteg.
5. wbStego4open.
6. Invisible Secrets.

These tools are available across the platforms such as LINUX, WINDOWS, MAC-OS, and UNIX. They also used various embedding algorithm as well as different types of cover image such as JPEG, BMP.

OutGuess: It inserts the hidden information into the redundant bits of data source. It is a universal steganographic tool. The program extracts the redundant bits and writes them back after modification. It uses JPEG images or PNM (Portable Any Map) files as cover images. The images will be used as concrete example of data objects, though OutGuess can use any kind of data, as long as a handler is provided.

StegHide: It is a steganographic tool that hides bits of a data file in some of the least significant bits of cover file. The existence of the data file is invisible and cannot be guessed. It is designed as portable. It hides data in ".bmp", ".wav" and ".au" files, blowfish encryption, MD5 hashing of passphrases to blowfish keys, and pseudo-random distribution of hidden bits in the container data.

JPHS: It refers Jpeg Hide and Seek. It uses lossy compression algorithm. It is available in both Windows and Linux versions. JPHS includes two programs JPHIDE and JPSEEK. JPHIDE.EXE hides a data file in Jpeg file. JPSEEK.EXE is used to recover the hidden file from Jpeg file. Since the hidden file is distributed to the Jpeg image the visual and statistical effects are very less. JPHS uses LSB methods for hiding information. It is designed in such a way that it is impossible to prove that the host file contains a hidden file. When the insertion rate is very less (under 5%), it is very difficult to know about the hidden data. As the insertion percentage increases the statistical nature of the jpeg coefficients differs from "normal" to the extent that it raises suspicion.

JSteg: It is more effective tool to hide data file into image file. It is being used as a best choice of hacker's community. It is the first

software used for embedding the data into JPEG image. Later, the JSteg-Shell was designed.

WbStego4open: It does not require registration. It is an open source application which works in Windows and Linux platform. Bitmaps, Text files, PDF files, and HTML files can be considered as carrier files. It is an effective tool for embedding copyright information without modifying carrier file.

Invisible Secrets: This tool is used to hide data in image or sound files. It provides extra protection by using AES encryption algorithm. During the creation of stego files, password is created and stored.

Other steganography tools: Some of the other tools used for image steganography comprises of Crypto123, Hermetic stego, IBM DLS, Invisible Secrets, Info stego, Syscop, StegMark, Cloak, Contraband Hell, Contraband, Dound, Gif it Up, S-Tools, JSteg_Shell, Blindside, CameraShy, dc-Steganograph, F5, Gif Shuffle, Hide4PGP, JstegJpeg, Mandelste, PGMStealth, Steghide.

2.5 IMAGE STEGANALYSIS

The counter-technique of image steganography is known as image steganalysis. It begins by identifying the artifacts that exist in the suspect file which has formed as a result of embedding a message. The goal is not to advocate the removal or disabling of valid hidden information such as copyrights, but to point out approaches that are vulnerable and may be exploited to investigate illicit hidden information (Anderson et al. [2]; Johnson et al. [55]; Neil et al. [81]; Rajarathnam et al. [90]). Attacks and analysis on hidden information may take several forms like detecting, extracting, and disabling or destroying hidden information, (Westfeld et al. [119]). An attacker may also embed counter-information over the existing hidden information. These

approaches vary depending upon the methods used to embed the information into the cover media.

Some amount of distortion and degradation may occur to carriers even though such distortions cannot be detected easily by the human perceptible system. This distortion may be anomalous to the normal carrier that when discovered may point to the existence of hidden information. Numerous tools exist in performing steganography, and they vary in their approaches for hiding information. The detection of hidden content is quite complex without knowing which tool is used and which, stego key is used. Some of the steganographic approaches have characteristics that act as signatures for the method or tool used.

2.5.1 Steganalysis Methods

Based on the way of detecting the presence of hidden message, steganalysis methods are divided as follows:

1. Statistical steganalysis.
    a. Spatial domain.
    b. Transform domain.
2. Feature based steganalysis.

Statistical steganalysis: In order to detect the existence of the hidden message, statistical analysis is done with the pixels. It is further classified as spatial domain steganalysis and transform domain steganalysis.

In spatial domain, the pair of pixels is considered and the difference between them is calculated. The pair may be any 2 neighboring pixels. They may be selected within a block otherwise across the two blocks. Finally the histogram is plotted that shows the existence of the hidden message.

In transform domain, frequency counts of coefficients are calculated and then histogram analysis is performed. With the help of this, the cover and stego images can be differentiated. However, this method is not providing information about the embedding algorithms. To overcome this problem, we may choose feature based steganalysis.

Feature based steganalysis: In this method, the features of the image will be extracted for selecting and retaining relevant information. These extracted features are used to detect hidden message in an image. They can also be used to train classifiers. This research focuses on feature based steganalysis.

2.5.2 Classification of steganalysis

The steganalysis algorithm may or may not depend on the steganographic algorithm (SA). Based on this, steganalysis is classified as follows:

1. Specific / Target steganalysis.
2. Generic / Blind / Universal steganalysis.

1. Specific steganalysis: The SA is known and the designing of detector (steganalysis algorithm) is based on SA. The steganalysis algorithm is dependent on the SA. This type of steganalysis is based on analyzing the statistical properties of an image that change after embedding. The advantage of using specific steganalysis is the results are very accurate. The disadvantage of using this method is it is very limited to particular embedding algorithm as well as the image format.

2. Blind / Universal steganalysis: In universal steganalysis, the SA is not known by everyone. Hence, anyone can design a detector to detect the presence of the secret message that will not depend on SA. Comparing with specific steganalysis, universal is common and less efficient. Still universal steganalysis is widely used than specific one

because it is independent of the SA. This research focuses on universal steganalysis. It includes the following 2 phases:

a. Feature Extraction.

b. Classification.

a. Feature Extraction: It is a process of creating a set of distinct statistical attributes of an image. These attributes are known as feature. Feature Extraction is nothing but a dimensionality reduction. The extracted features must be sensitive to the embedding artifacts. Image quality metrics, wavelet decompositions, moment of image statistic histograms, Markov empirical transition matrix, moment of image statistic from spatial and frequency domain, co-occurrence matrix are some of the feature extraction methods.

b. Classification: It is a way of categorizing the images into classes depending on their feature values. Supervised learning is one of the primary classifications in steganalysis. Supervised learning allows learning under some supervision. In this learning, a set of training inputs that includes input features is given as input to train the classifier. After the training, class label is predicted based on the features that are given. steganalysis use the following classifiers:

1. Multivariate regression.
2. Fisher linear discriminant (FLD).
3. Support vector machine (SVM).
4. Artificial neural network (ANN).

1. Multivariate regression: It consists of regression co-efficient. In the training phase, regression coefficients are predicted using minimum mean square error.

2. FLD: It is a linear combination of features which maximizes the separations. In the classification method, multi dimensional features are projected into a linear space.

3. SVM: This classification method learns from the given sample. It is trained to recognize and assign class labels based on a given set of features.

4. ANN: It is defined as an information processing model that simulates biological neuron system. It includes collection of PE, similar to neuron. Feed forward and back propagation neural networks are commonly used in classification. The classification process has 2 steps, training and testing. In a training phase, the neural network associates the outputs with the given input patterns, by modifying the weights of inputs. In a testing phase, the input pattern is identified and the associated output is determined. This thesis uses ANN classifier for detecting the presence of hidden information.

2.5.3 Steganalysis tools

Various steganalysis tools are available to detect the presence of hidden information with the stego image. Some of the steganalysis tools are mentioned below:

1. StegDetect.
2. StegSecret.
3. JPSeek.
4. StegBreak.

StegDetect: It is an automated tool for detecting steganographic content in images. It is capable of detecting several different steganographic methods to embed hidden information in JPEG images. Currently, the detectable schemes are jsteg, jphide, invisible secrets; OutGuess 01.3b, F5, appendX, and camouflage. Using linear discriminant analysis, it also supports detection of new stego systems.

JPSeek: It is a program that allows detecting the hidden massage inside a jpeg image. There are various versions of similar programs available

on the internet but JPSeek is rather special. The design objective is same as JPHide.

StegSecret: It is a steganalysis open source project that makes possible the detection of hidden information in different digital media. StegSecret is java-based multiplatform steganalysis tool that allows the detection of hidden information by using the most known steganographic methods. It detects EOF, LSB, and DCT like techniques.

StegBreak: It launches brute-force dictionary attacks on JPG image. The StegBreak states a brute-force dictionary attack against the specified JPG images.

Other steganalysis tools: Some more image steganalysis tools are 2Mosaic, StirMark Benchmark, Phototile, StegSpy, Stego Suite, Steganalysis Analyzer Real-Time Scanner, JSteg detection, JPHide detection, OutGuess detection.

2.6 REAL TIME APPLICATIONS OF STEGANALYSIS IN OTHER FIELDS

a. **Medical safety**: Current image formats such as DICOM separate image data from the text (such as patients name, date and physician), with the result that the link between image and patient occasionally gets mangled by protocol converters. Thus embedding the patients name in the image could be a useful safety measure.
b. **Terrorism**: According to government officials terrorists use to hide maps and photographs of terrorist targets and giving instructions for terrorists targets.
c. **Hacking**: The hacker hides a monitoring too, server behind any image or audio or text file and shares it with mail or chat which will get installed and executed which will help the hacker to do anything with the workstation.

d. **Intellectual property offenses**: Intellectual property, defined as the formulas, prototypes, copyrights and customer lists maintained by a company, can be far more valuable than the actual items they sell.
e. **Corporate espionage**: Usage of spies to collect information about what another entity is doing or planning in a corporate environment.
f. **Watermarking**: Special inks to write hidden messages on bank notes and also the entertainment industry using digital watermarking and fingerprinting of audio and video for copyright protection.
g. **Indexing of video mail**: Embed comments in the content.
h. **Military application**: Very much used during war times.
i. **Automatic monitoring of radio advertisements:** It would be convenient to have an automated system to verify that adverts are played as contracted.

2.7 ARTIFICIAL NEURAL NETWORKS

ANN is a mathematical model that simulates the structure and functional aspects of biological neural network. In other words it is an emulation of biological neural system. ANN mimics some features of a real nervous system that contains a collection of basic computing units called "neurons". These are the basic signaling units of the nervous system. Each neuron is a discrete cell whose several processes arise from its cell body. These neurons were represented as models of biological networks into conceptual components for circuits that could perform computational tasks. The basic model of the neuron is founded upon the functionality of a biological neuron.

ANN consists of an interconnected group of artificial neurons and processes information using a connectionist approach for computation. Such model shows strong resemblance to axons and dendrites in a nervous system. Robustness, flexibility and collective computation are

the attractive features of this model, due to its self-organizing and adaptive nature. An artificial functional model of the biological neuron includes three basic components. First the synapses of the biological neuron are modeled as weights. The synapse of the biological neuron interconnects the neural network and gives the strength of the connection. For an artificial neuron, the weight is a number, and represents the synapse. A negative weight reflects an inhibitory connection, while positive values designate excitatory connections. All inputs are summed altogether and modified by the weights. This is referred as a linear combination. Finally, an activation function controls the amplitude of the output. For example, an acceptable range of output is usually between 0 and 1, or it could be -1 and 1.

The nodes of the networks resemble differential equations. The connections between these nodes can either be inter-connected among adjacent layers or intra-connected with adjacent neurons in the same layer. Activation value obtained from previous layer is fed into the nodes of the successive layers. The activation value is the output of activation function from connection weights of previous layer. The activation value is passed through a non linear function. The operation of a neuron is shown in figure 2.4.

Hard-limiting nonlinearity is considered, if vectors are binary or bipolar and a squashed function is chosen, if vectors are analog in nature. Popular squashed functions are sigmoid (0 to 1), tanh (-1 to +1), Gaussian, logarithmic and exponential. A network can either be discrete or analog. The neuron of a discrete network is associated with two states, whereas the analog network is associated with a continuous output. Discrete network can be synchronous, when the state of every neuron in the network is updated. In the same way, it can be asynchronous, when only one neuron is updated for a given time period.

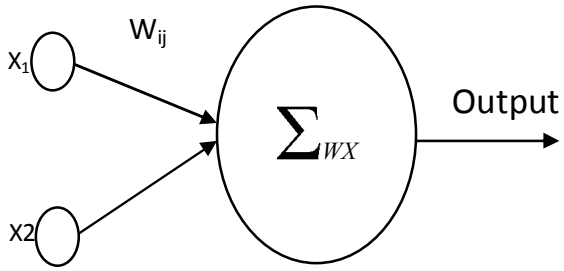

Fig. 2.4 Operation of a neuron

A feed forward network provides input to the next layer with no closed chain of dependence among neural states through a set of connection strengths or weights. The chain has to be closed to make it feedback network. When the output of the network depends upon the current input, the network is static (no memory). If the output of the network depends upon past inputs or outputs, the network is dynamic (recurrent). If the interconnection among neurons changes with time, the network is adaptive; otherwise it is called non-adaptive.

In reality, most of the patterns are not linearly separable. Non linear classifiers are used for pattern classification, in order to achieve good separability. The multilayer network is a non linear classifier, since it uses hidden layer. In addition to multiplayer network, polynomial discriminate function (PDF) is also a non linear classifier. In the PDF, the input vector is pre-processed. Normally, neural networks are used for classify patterns by learning from samples. Different neural network paradigms employ different learning rules. In some way, all these paradigms determine different pattern statistics from a set of training samples. Then, the network classifies new patterns on the basis of these statistics.

Various weight updating methods have been developed to learn the patterns by the neural networks. They are classified as supervised methods and unsupervised methods. Since both the inputs and outputs

are considered, supervised learning technique has been used. The unsupervised methods use only inputs and no target outputs. A neuron is said to be fired, if the sum of its excitatory inputs reach its threshold value. This state remains valid, until neuron receives no inhibitory input. This model can be used to construct a network which has the ability to compute any logical function. But this model was unbiological. To overcome the deficiencies of this model, a new model named perceptron model was proposed, which could be utilized to learn and generalize. In addition to the above two types of learning, the concept of supervised learning was developed and incorporated in the adaptive linear element model (ADALINE).

The present work involves modification of existing weight updating algorithm, combination of classical method with neural network method of training the network for more number of patterns, and training the network properly for more than two classifications. The performance of the different methods developed and trained has been compared with the performance of BPA, since BPA is a well known algorithm. The network functions on a supervised learning strategy. The inputs of a pattern are presented. The output of the network obtained in the output layer is compared with the desired output of the pattern. The difference between the calculated output of the network and the desired output is called the Mean Squared Error (MSE). The MSE of the network for the pattern presented is minimized. This error is propagated backwards, such that the weights connecting the different layers are updated. By this process, the MSE of the network for the pattern presented is minimized. This procedure has to be adopted for all the training patterns and the MSE of each pattern is summed up. After presenting the last training pattern, the network is considered to have learnt all the training patterns through iterations, but the MSE is large.

To minimize MSE, the network has to be presented with all the training patterns many times. There is no guarantee that the network will reach the global minimum; instead, it will reach one of the local minima. The MSE may increase, which means divergence rather than convergence. Sometimes, there may be oscillation between convergence and divergence. The training of the network can be stopped either by considering MSE or by considering prediction performance as the criterion. When prediction performance is considered as the criterion, test patterns are presented at the end of iteration. Once the desired performance is obtained, training of the network is stopped. When MSE is considered as the criterion, one may not know the exact MSE, to which the network has to be trained. If the network is trained till it reaches a very low MSE, over-fitting of the network occurs. Over-fitting represents the loss of generality of the network. That is, the network classifies only the patterns, which are used during training, and not the test patterns. The detailed review of literature for steganalysis using ANN is given in section 2.8.11.

2.8 REVIEW OF LITERATURE

2.8.1 Visual attacks

The visual attacks (Westfeld et al. [121]) detect the steganography by making use of the ability of human eyes to inspect the images for the corruption caused by the embedding.

2.8.2 Pairs analysis

Pairs analysis was proposed (Fridrich et al. [30]). This approach is well suited for the embedding archetype that randomly embeds messages in LSBs of indices to palette colors of palette image.

2.8.3 F5 embedding algorithm

The F5 algorithm was introduced by German researchers (Westfeld [120]). It embeds message bits into non-zero AC coefficients and adopts matrix encoding to achieve the minimal number of changes in quantized coefficients during embedding process. The matrix encoding is the core of the F5 algorithm. It is determined by the message length and the number of non-zero AC coefficients. It can be represented as the form (c, n, and k). The parameter c tells how many coefficients at most will be modified during embedding, and n is the number of coefficients involved in embedding the k-bit message. In the embedding process, the message is divided into segments of k bits to embed into a group of n randomly chosen coefficients. F5 algorithm manipulates the quantized coefficients when the hash of that group does not match the message bits, thus the histogram values of DCT coefficients are modified. For example, if the shrinkage occurs, the number of zero AC coefficients will increase and the number of remaining non-zero coefficients decreases with embedding. The changes in the histogram of DCT coefficients may be utilized to detect the presence of hidden message.

2.8.4 RS steganalysis

Fridrich et al. [35] developed a steganalytic technique based on this for detection of LSB embedding in color and grayscale images. They analyze the capacity for embedding lossless data in LSBs. Randomizing the LSBs decreases this capacity. To examine an image, they define Regular groups (R) and Singular groups (S) of pixels depending upon some properties. Then with the help of relative frequencies of these groups in the given image, in the image obtained from the original image with LSBs flipped and an image obtained by randomizing LSBs of the original image, they try to predict the levels of embedding.

2.8.5 DCT domain steganalysis

Many steganalysis researchers such as Neil et al. [80] attempt to categorize steganalysis attacks to recover modify or remove the message, based on information available. The steganalysis technique developed can detect several variants of spread-spectrum data hiding techniques (Marvel et al. [73]). The first steganalysis technique using wavelet decomposition was developed (Farid [21]). Fridrich et al. [25], [30] have shown that this change is proportional to the level of embedding. They also showed that, if an image is cropped by 4 rows and 4 columns, then original DCT histogram can be obtained.

The basic assumption here is that the quantized DCT coefficients are robust to small distortions and after cropping the newly calculated DCT coefficients will not exhibit clusters due to quantization. Also, because the cropped stego image is visually similar to the cover image, many macroscopic characteristics of cover image will be approximately preserved. After predicting DCT coefficient's histogram in the original image and comparing with that of a stegoed image, the hidden message length can be calculated. Sullivan et al. [82] use an empirical matrix as the feature set to construct a steganalysis. Chen et al. [14] enhanced and applied the statistical moments on JPEG image steganalysis.

2.8.6 Detecting LSB hiding

An early method used to detect LSB hiding is the 2 (chi-squared) technique later successfully used to stegdetect for detection of LSB hiding in JPEG coefficients. Another LSB detection scheme was proposed by (Avcibas et al. [5]), using binary similarity measures between the 7^{th} bit plane and the 8^{th} (least significant) bit plane. It is assumed that there is a natural correlation between the bit planes that is disrupted by LSB

hiding. This scheme does not auto-calibrate on a per image basis, and instead calibrates on a training set of cover and stego images. The scheme works better than a generic steganalysis scheme, but not as well as state-of-the-art LSB steganalysis.

Another LSB detection scheme was proposed using binary similarity measures between the 7^{th} bit plane and the 8^{th} (least significant) bit plane. It is assumed that there is a natural correlation between the bit planes that is disrupted by LSB hiding. This scheme does not auto-calibrate on a per image basis, and instead calibrates on a training set of cover and stego images. The scheme works better than a generic steganalysis scheme, but not as well as state-of-the-art LSB steganalysis.

Scheme, proposed by Fridrich et al. [27] is a specific steganalysis method for detecting LSB data hiding in images. Sample pair analysis is a more rigorous analysis due to (Dumitrescu et al. [19]) of the basis of the RS method, explaining why and when it works. Roue et al. [92] uses estimates of the joint probability mass function (PMF) to increase the detection rate of RS/sample pair analysis. Fridrich et al. [26] uses local estimators based on pixel neighborhoods to slightly improve LSB detection over RS.

2.8.7 Detecting other hiding methods

Harmsen et al. [45] proposed steganalysis of additive hiding schemes such as spread spectrum. Their decision statistic is based initially on a PMF estimate called histogram. Since additive hiding is an addition of two random variables: the cover and the message sequence, the PMF of cover and message sequences are involved. In the Fourier domain, this is equivalent to multiplication. Therefore the DFT of the histogram, termed the histogram characteristic function (HCF), is taken.

It is shown for typical cover distributions that the expected value or center of mass (COM), of the HCF does not increase after hiding, and in practice typically decreases. The authors choose then to use the COM as a feature to train a Bayesian multivariate classifier to discriminate between cover and stego. They perform tests on RGB images, using a combined COM of each color plane, with reasonable success in detecting additive hiding.

Fridrich's et al. [30] content-independent stochastic modulation is statistically identical to spread spectrum and Celik et al. [9] proposed using rate-distortion curves for detection of LSB hiding. They observe that data embedding typically increases the image entropy, while attempting to avoid introducing perceptual distortion to the image. On the other hand, compression is designed to reduce the entropy of an image while also not inducing any perceptual changes.

It is expected therefore that the difference between a stego image and its compressed version is greater than the difference between a cover and its compressed form. Distortion metrics such as MSE, mean absolute error, and weighted MSE are used to measure the difference between an image and compressed version of the image. A feature vector consisting of these distortion metrics for several different compression rates (using JPEG2000) is used to train a classifier. False alarm and missed detection rates are each about 18%.

2.8.8 Generic steganalysis

The following schemes are designed to detect any arbitrary scheme. Instead of classifying cover images and images with LSB hiding, they discriminate between cover images and stego images with any hiding scheme, or class of hiding schemes. The underlying assumption is that cover images posses some measurable naturalness that is disrupted

by adding data. In some respects this assumption lies at the heart of all steganalysis. To calibrate the features chosen to measure "naturalness", the systems learn using some form of supervised training.

An early approach was proposed by (Avcibas et al. [7]) to detect arbitrary hiding schemes. He design a feature set based on image quality metrics (IQM), metrics designed to mimic the human visual system (HVS). In particular they measure the difference between a received image and a filtered (weighted sum of 3 × 3 neighborhood) version of the image. This is very similar in spirit to the work by (Celik et al. [9]) except with filtering instead of compression. The key observation is that filtering an image without hidden data changes the IQMs differently than an image with hidden data. The reasoning here is that the embedding is done locally (either pixel-wise or block wise), causing localized discrepancies.

A supervised learning has been used to detect general steganalysis (Lyu et al. [68]). Lyu et al. [67] use a feature set based on higher-order statistics of wavelet sub band coefficients for generic detection. The earlier work used a two-class classifier to discriminate between cover and stego images made with one specific hiding scheme. Later work however uses a one class, multiple hyper sphere, SVM classifier. The single class is trained to cluster clean cover images. Any image with a feature set falling outside of this class is classified as stego. In this way, the same classifier can be used for many different embedding schemes. The one-class cluster of feature vectors can be said to capture a "natural" image feature set. As with Avcibas et al. [5], the general applicability leads to a performance hit in detection power compared with detectors tuned to a specific embedding scheme. However the results are acceptable for many applications.

Martin et al. [71] attempts to directly use the notion of the naturalness of images to detect hidden data. Though they found that data hidden certainly caused shifts from the natural set, knowledge of the specific data hiding scheme provides far better detection performance. Fridrich et al. [26] presented supervised learning method tuned to JPEG hiding schemes. The feature vector is based on a variety of statistics of both spatial and DCT values. The performance seems to improve over previous generic detection schemes by focusing on a class of hiding schemes (Kharrazi et al. [59]).

2.8.9 Evading steganalysis

Another steganographic scheme has been based on LSB hiding, but designed to evade the chi square test (Provos [86]). Here, LSB hiding is done as usual (again in JPEG coefficients), but only half the available coefficients are used. The remaining coefficients are used to compensate for the hiding, by repairing the histogram to match the cover. Although the rate is lower than F5 hiding, since half the coefficients are not used, but by Fridrich et al. [27] F5 detector, and in fact by any detector using histogram statistics. However, because the embedding is done in the block wise transform domain, there are changes in the spatial domain at the block borders. Specifically, the change to the spatial joint statistics, i.e. the dependencies between pixels, is different than for standard JPEG compression.

Due to the success of steganalysis in detecting early schemes, new steganographic methods have been invented in an attempt to evade detection. F5 by (Westfeld [120]) is a hiding scheme that changes the LSB of JPEG coefficients, but not by simple overwriting. By increasing and decreasing coefficients by one, the frequency equalization noted in standard LSB hiding is avoided. That is, instead of standard LSB hiding,

where an even number is either unchanged or increased by one and an odd is either unchanged or decreased by one, both odd and even numbers are increased and decreased. This method does indeed prevent detection by the 2 test.

However, (Fridrich et al. [25]) note that although F5 hiding eliminates the characteristic "step-like" histogram of standard LSB hiding, it still changes the histogram enough to be detectable. A key element in their detection of F5 is the ability to estimate the cover histogram. As mentioned above, the 2 test only estimates the likelihood of an image being stego, providing no idea of how close it is to cover. By estimating the cover histogram, an unknown image can be compared to both an estimate of the cover, and the expected stego, and whichever is closest is chosen. Additionally, by comparing the relative position of the unknown histogram to estimates of cover and stego, an estimate of the amount of data hidden, the hiding rate can be determined. The method of estimating the cover histogram is to decompress, crop the image by 4 pixels (half a JPEG block), and recompress with the same quantization matrix (quality level) as before.

Fridrich et al. [25] were able to exploit these changes at the JPEG block boundaries again using a decompress crop recompress method of estimating the cover (joint) statistics; they are able to detect OutGuess and estimate the message size with reasonable accuracy. Eggers et al. [20] suggest a method of data-mappings that preserve the first order statistics, called histogram-preserving data-mapping (HPDM). As with the method proposed by Franz, the distribution of the message is designed to match the cover, resulting in a loss of rate.

Fridrich et al. [30] find this cropped and recompressed image is statistically very close to the original, and generalize this method to detection of other JPEG hiding schemes. Tzschoppe et al. [111] suggest

a minor modification to avoid detection: basically not hiding in perceptually significant values. Fridrich et al. [30] propose the stochastic modulation hiding scheme designed to mimic noise expected in an image. The non-content dependent version allows arbitrarily distributed noise to be used for carrying the message. If Gaussian noise is used, the hiding is statistically the same as spread spectrum, though with a higher rate than typical implementations. The content dependent version adapts the strength of the hiding to the image region.

2.8.10 Detection-theoretic analysis

An example of a detection-theoretic approach to steganalysis is (Cachin et al. [8]). The steganalysis problem is framed as a hypothesis test between cover and stego hypotheses. Cachin suggests a bound on the Kullback-Leibler (KL) divergence (relative entropy) between the cover and stego distributions as a measure of the security between cover and stego. Another information theoretic derivation is done for a slightly different model by (Zolner et al. [144]). They first assume that the steganalyst has access to the exact cover, and prove the intuition that this can never be made secure. They modify the model so that the detector has some, but not complete information on the cover. From this model they find constraints on conditional entropy similar to Cachin [8] though more abstract and hence more difficult to evaluate in practice.

Westfeld et.al [119] proposed raw image steganalysis based on the assumption that the message length should be comparable to the pixel count in the cover image. Detection theory is well developed and has been applied to a variety of fields and applications (Provos [86]). Its key advantage for steganalysis is the availability of results prescribing optimal (error minimizing) detection.

Chandramouli et al. [10] use a detection-theoretic framework to analyze LSB detection. Guillon et al. [41] analyze the detecting ability of QIM steganalysis, and observe that QIM hiding in a uniformly distributed cover does not change the statistics. Since typical cover data is not in fact uniformly distributed, they suggest using a non linear "compressor" to convert the cover data to a uniformly distributed intermediate cover. The data is hidden into this intermediate cover with standard QIM, and then the inverse of the function is used to convert to final stego data. Farid [22] explained about the usage of higher order statistics for generic steganalysis techniques and the first order statistics for the specific steganalysis techniques. Fridrich [30] explained a technique for estimating the unaltered histogram to find the number of changes and length of secret message.

Sidorov [104] presented work done on using hidden Markov model (HMM) theory for the study of steganalysis. He presents analysis on using Markov chain and Markov random field models, specifically for detection of LSB. Though the framework has great potential, the results reported are sparse. He found that a Markov chain (MC) model provided poor results for LSB hiding in all but high-quality or synthetic images, and suggested a Markov random field (MRF) model, citing the effectiveness of the RS/sample pair scheme.

Sallee [94] proposed a means of evading optimal detection. The basic idea is to create stego data with the same distribution model as the cover data. That is, rather than attempting to mimic the exact cover distribution, mimic a parameterized model. The justification for this is that the steganalyst does not have access to the original cover distribution, but must instead use a model. A specific method for hiding in JPEG coefficients using a Cauchy distribution model is proposed.

Detection theory to steganalysis is Hogan et al. [47] QIM (quantization index modulation) steganalysis. Hernandez et al. [46] proposed a global steganalysis methodology by comparing some of the steganalysis methods. Using stego images generated by typical data hiding algorithms, the secret message detection capacities of these steganalysis methods are evaluated. The evaluation of steganalysis methods is represented in terms of false negative and false positive error rates using 100 images. Chao et al. [13] proposed a method based on the good property of fractional Fourier transform (FRFT) coefficients of image histogram for extracting two kinds of features of an image. SVM is used as a classifier.

Mei et al. [76] introduced an alpha-trimmed method as an image estimation technique for distinguishing cover and stego images. This method estimates steganographic messages within images in the spatial domain that provides flexibility for classifying various steganalysis methods in the JPEG compression domain. Wang et al. [23] used a new kind of transition probability matrix is constructed to describe correlations of the quantized DCT coefficients in the multi-directions. Subsequently, 96-dimensional feature vector is extracted by merging two different calibrations. SVM is trained to build the steganalyzer.

Zhiping Zhou et al. [139] developed zigzag scanning pattern to arrange both DCT blocks and coefficients in each block. The computational complexity of the proposed method is manageable with the help of Threshold and truncation techniques. Bidirectional Markov matrix is exploited to capture the correlations between the adjacent coefficients in both intra-block and inter-block senses, which have been changed during data embedding. Features for steganalysis are derived from intra-block and inter-block Markov transition matrixes.

Qian-lan et al. [88] proposed an image steganalysis scheme based on the differential image histogram in frequency domain. The difference is calculated in three directions, horizontal, vertical and diagonal towards adjacent pixels to obtain three-directional differential images for a natural image. The features for steganalysis are extracted from the DFT of the histogram of differential images and divided into low and high frequency bands. SVM with RBF kernel is applied as classifier.

Xiaoyuan et al. [129] used Wavelet based Markov Chain (WBMC) model for nature images. It presents statistic divergence between cover image and steg image prominently. Based on Markov chain empirical matrix, the difference between low frequency domain and high frequency domain generalized by steg process is discussed. It also defined two models: WBMC_L model and WBMC_H model respective to construct WBMC model. Wenqiong et al. [116] constructed nine statistical models from the DCT and decompressed spatial domain for a JPEG image. Feature set is measured by calculating the histogram characteristic function (HCF) and the center of mass (COM). SVM are used as classifiers.

Seongho Cho et al. [95] classify the image blocks into multiple classes on steganalysis that provides decomposed image blocks. Also it uses a classifier for each class to decide whether a block is from a cover or stego image. Consequently, the steganalysis of the whole image can be performed by fusing steganalysis. Jingwei Wang et al. [96] design a multi-classifier which classifies stego images depending on their steganographic algorithms. Based on steganalysis results of decomposed image blocks stego image is distinguished from cover images.

Yamini et al. [133] calculated the length of embedded message using SVM as a classifier. Zhi-Min et al. [138] proposed a RBF Neural Network (RBFNN) optimized by the Localized Generalization Error Model

(L-GEM) for steganography detection. Discrete cosine transform (DCT) features and the Markov features are given as inputs of neural networks. They enhance the generalization capability of the RBFNN and the performance of detecting steganalysis in future images. The architecture of the RBFNN is selected by minimizing the L-GEM.

Ramezani et al. [91] compared Fisher linear discriminant (FLD), Gaussian naïve Bayes, multilayer perceptron, and k nearest neighbor for steganalysis of suspicious images. The method exploits statistics of the histogram, wavelet statistics, amplitudes of local extrema from the ID and 2D adjacency histograms, center of mass of the histogram characteristic function and co-occurrence matrices for feature extraction process. In order to reduce the proposed features dimension and select the best subset, genetic algorithm is used and the results are compared through principle component analysis and linear discriminant analysis.

Gireesh Kumar et al. [40] compared the efficiency of two embedding algorithms using the image features that are consistent over a wide range of cover images, but are distributed by the presence of embedded data. Image features were extracted after wavelet decomposition of the given image. These features were then given to a SVM classifier to identify. Holoska et al. [48] compared universal neural network classification and a linear classification tool (Stegdetect). Based on the results it is concluded that neural networks were better than the linear classification tool. Sheikhan et al. [100] extracted the features from Contourlet coefficients and co occurrence metrics of sub band images. Analysis of Variance (ANOVA) method is used to reduce the number of features. The selected features are fed to nonlinear SVM for classification.

Ke Ke et al. [58] explore Bhattacharyya Distance principle to recognize stego algorithms that are being used. The most important

features are selected by the means of applying Bhattacharyya distance. BPA is used to classify cover and stego images. Chen Qunjie et al. [15] proposed a steganographic detection method for JPEG image which is based on the data-dependent concept. The initial classifier is obtained by SVM training. Then the kernel function is modified with conformal transformation by using the information of Support Vectors and retrain with the new kernel to enlarge the spacing around classification boundary. Repeat this until the best result is obtained.

Li Hui et al. [61] proposed the scheme based on the characteristic function (CF) moments of three-level wavelet sub bands as well as the further decomposition coefficients of the first scale diagonal sub band. The first three statistical moments of each wavelet band of test image and prediction-error image are selected to form 102 dimensional features for steganalysis. Principal Components Analysis (PCA) is utilized to reduce the features. SVM is adopted as the classifier.

Ping et al. [116] proposed a novel method for universal steganalysis on frequency domain to detect hidden message. The detection is achieved based on the spectrum analysis of difference histogram of frequency coefficients according to evident spectrum difference between cover images and stego images. Experimental results from detecting steganographic images of DCT domain and DWT domain show that the detection performance is satisfied.

2.8.11 Steganalysis using ANN

Supervised learning methods construct a classifier to differentiate between stego and non stego images using training examples. Supervised learning methods using neural networks as classifiers, gained much importance in recent studies on steganalysis (Liu et al. [65]; Shi et al. [101]; Ryan et al. [93]; Muhanna et al. [79]; Qingzhong et al. [89];

Ying et al. [134]; Mei et al. [75]; Yuan et al. [135]; Lingna et al. [64]; Ferreira et al. [24]; Han et al. [44]; Xiongfei et al. [131]; Ziwen et al. [141]; Malekmohamadi et al. [70]) Describing the supervised learning steganalysis method in a general scenario, some image features are first extracted and given as training input to a learning machine. These examples include both stego and non stego messages. The learning classifier iteratively updates its classification rule based on its prediction and the ground truth. Upon convergence the final stego classifier is obtained. Some of the major advantages using supervised learning based steganalysis are as follows:

1. Construction of universal steganalysis detectors using learning techniques and
2. Several freely available software packages on the Internet could be directly used to train a steganalysis detector.

Martin et al. [72] found that data hidden certainly caused shifts from the natural set, knowledge of the specific data hiding scheme provides far better detection performance. A variation of passive steganalysis is active steganalysis, deals in determining or estimating the length of the secret message and the extraction of actual contents of the message (Chandramouli et al. [11]; Fridrich et al. [30]; Chandramouli [12]; Jacob et al. [54]; Ming et al. [78]; Shaohui et al. [99]; Xiangyang et al. [44]). The methods that estimate the length of secret message or extract the hidden contents are known as embedding- specific methods. A universal or generic steganalytic method that should be independent of embedding-specific method suits best in digital forensics.

Most of the present literature on steganalysis follows either a blind model (Farid [22]; Jacob et al. [54]; Lyu [67]; Celik et al. [9]; Guo [43]; Hongchen et al. [50]; Chen et al. [14]; Gul et al. [42]; Zhuo et al. [140]; Xiao et al. [125]; Xue et al. [132]; Wang et al. [23]; Feng et al.

[13]) or a parametric model [Harmsen et al. [45]; Tariq et al. [110] ; Hong et al. [49]; Yun et al. [136]; Wu et al. [141]; Liang et al. [63]).

Stating in other terms the present steganalytic work fall broadly into one of two categories: the embedding-specific steganalysis that take advantage of particular algorithmic details of the embedding algorithm, and generic steganalysis that attempts to detect the presence of an embedded message independent of the embedding algorithm and, ideally, the image format. Significant work has been done in detecting steganalysis using image statistical observations [Zhang et al. [137]; Xiangyang et al. [123]; Anderson et al. [1]; Tao et al. [109]]. For instance, LSB insertion in raw pixels results in specific changes in the image grayscale histogram, which can be used as the basis for its detection. However, given the ever growing number of steganalysis tools, embedding-specific approaches are clearly not suitable in order to perform generic and, large-scale steganalysis.

On the other hand, though visually hard to differentiate, the statistical regularities in the natural image as the steganography cover are disturbed by the embedded message. For instance, changing the LSBs of a grayscale image will introduce high frequency artifacts in the cover images. The difference between a clean and a stego image in the high frequency region, presents the artifacts introduced by the embedding. The generic steganalysis detects steganography by capturing such artifacts. A framework for steganalysis based on supervised learning has been designed. The framework was further developed and tested by many researchers. The general framework for generic image steganalysis is followed in the work based on discriminative image features from linear and non linear classification techniques. Without the knowledge of the embedding algorithm, the proposed work detects steganography.

2.8.12 Limitations in steganalysis

Although there are some techniques that can detect steganography there are major problems that steganalysts face. Even if there are noticeable distortions and noise, predictable patterns cannot always be detected. Some steganographic techniques are particularly difficult to detect without the original image. And in most cases, it is highly unlikely that a forensic investigator will be conveniently presented with the steganographic and original image. Even until today, most steganalysis techniques are based on visual attacks and methods beyond this are being explored. Unfortunately a general steganalysis technique has not been devised (Johnson et al. [55]).

While visual attacks are more prominent, JPEG images, which is one of the most commonly distributed type of image format; the steganographic modifications take place in the frequency domain. This means that this type of steganography is not susceptible to visual attacks unlike in image formats such as GIF images where the modifications happen in the spatial domain Provos et al. [85]; Niel Provos et al. [81] created a cluster that scans images from newsgroups to detect steganographic content in order to verify the claims about terrorists with the help of Internet to distribute secrets using steganography. For reasons that no hidden messages were discovered, it raises the question of the practicality of such detection systems (Krenn [60]).

2.8.13 Feature extraction for steganalysis

Xiaochuan Chen et al. [163] used statistical analysis of empirical matrix (EM) to detect the hidden message in an image. With the help of projection histogram of EM, moments of PH and the moments of the

characteristic function of PH features are extracted. To enhance the performance, features extracted from prediction-error image are also included. SVM is used as a classifier.

Yuan Liu et al. [135] proposed three methods for deriving the feature vector such as Robert gradient energy in pixel domain, variance of Laplacian parameter in DCT domain and higher-order statistics extracted from wavelet coefficients. BPA neural network is applied as the classifier.

Xiangyang Luo et al. [164] used WPT to decompose image into three scales and obtained 85 coefficient sub bands together. Multi-order absolute characteristic function moments of histogram are extracted from these sub bands as features. Finally these features are normalized and combined to a 255-D feature vector for each image. Back-propagation neural network is used as a classifier.

Yuan-lu Tu et al. [166] proposed a method for feature extraction by calculating the features from the luminance and chrominance components of the images. Features are extracted both in DCT and DWT domains. Wavelet high-order statistics is substituted with the moments of wavelet characteristic function. Non linear SVM classification is implemented.

Jing-Qu Lin et al. [165] proposed Binary Similarity Method (BSM) for capturing the seventh and eighth bit planes of the non-zero DCT coefficients from JPEG images and 14 features of each image are computed. SVM is used as a classifier. Zhi-Min He et al. [167] used RBFNN for steganalysis. DCT features and the Markov features are used as inputs of neural networks.

Sheikhan et al. [100] proposed a method for extracting features from Contourlet coefficients and co occurrence metrics of sub band images. Analysis of Variance (ANOVA) method is used and hence the

number of features is reduced. Non linear SVM is used as a classifier. Lie et al [168] used the gradient energy and statistical variance as two features for detecting the presence of hidden messages in spatial or DCT domain. Shi et al. [102] proposed a method that uses statistical moments of characteristic functions of the prediction-error image, the test image, and their wavelet sub bands as selected features. ANN is used as classifier.

2.9 SUMMARY

This chapter has presented an overview of various types of steganography and steganalysis methods. Some of the steganographic and steganalysis tools are discussed. Limitations of steganalysis as well as review of literature on steganalysis are also described. Generation of data is described in chapter 3.