CHAPTER 1
INTRODUCTION

With the latest development in information technology and the high usage of data on Internet, the need for information security has increased in the recent past. There are two main branches of information security – Cryptology and Data Hiding. Both these branches have fascinated people since centuries and numerous studies have tried to unravel their mysteries. Cryptology is a combination of two areas: Cryptography and Cryptanalysis. Cryptography is the study of schemes used for encryption and Cryptanalysis is the study of techniques used for deciphering a message with no knowledge of enciphering. Cryptology has traditionally been used for security, privacy or confidentiality of communication over an insecure channel (Stalling, 2012). Since the encrypted data is unreadable, it is not hidden from the eavesdroppers. There has been a tremendous advancement of computing power which has made it easier to break this secure communication. For this reason, data hiding techniques have emerged as an alternative to achieve secure communication. Data hiding can be defined as the art and science of hiding (or embedding) data into information file so that the existence of data is concealed to the eavesdroppers. This field has been an important and interesting discipline of information security since the early 1990s. It has emerged as a useful field for resolving the problems of public network security and secure communications. It can be used for wide range of applications for the safe circulation of secret data in e-Government, Military/ Defense, intelligence agencies. It can also be used for security of transmitting data and recovery of original cover for medical profession and law enforcement fields. For the organizations such as Banking, Commerce, Diplomacy and Medicine, the private communications is essential.

Amongst various methods of data hiding, Steganography and Watermarking are two techniques used to protect the sensitive data in original form. The modern digital Steganography is the art of hiding data within a digital cover object so that it is undetectable by the eavesdropper. The main goal of steganography includes hiding
information in undetectable way both perceptually and statistically. Digital Watermarking, on the other hand, is used to protect the digital medium from illegal copying, tamper proofing, copyright violation and unauthorized modifications. The information embedded inside the cover object usually is small. Error correction codes (ECCs) which is commonly used for detecting and correcting errors in data transmission has emerged as a new data hiding protocol to increase the security of data hiding scheme. In fact, the ECCs is mostly used in conjunction with data hiding and cryptography to reconstruct the embedding bit string after the re-encoding.

The basic concepts of Image Steganography are reviewed in Section 1.1. In Section 1.2 we have discussed the problems that have motivated us to work in this area. After introducing the data hiding problems we summarize our contributions in the field of image steganography in Section 1.3. Next we present the brief outlines of steganographic schemes that have been referred in the thesis for developing algorithms. To evaluate the performance of proposed algorithms on image steganography we have used widely acceptable metrics defined in Section 1.6. Finally we have concluded the summary of each chapter given in this thesis in Section 1.7.

1.1. OVERVIEW OF IMAGE STEGANOGRAPHY

Amongst many carriers such as a text file, image file, audio/video file or a TCP/IP header file, that have a high degree of redundancy, image file is found to be a most popular cover object due to its confined ability of human visual system, ‘innocent’ data types to eavesdroppers and availability of high degree of redundancy (Amirtharajan et. al., 2012). For example, a 1024 x 768 image has a potential to hide a total of 294,912 bytes of information using 3-LSB insertion method. In 640 x 480 image of 256 colors (8 bits/pixel), one can hide 300 KB worth of data and it is possible to hide 15% to 20% of data in a jpeg successfully (Ortiz, 2011). Further, digital images are the most common on the Internet. The images are also found to be one of the best cover objects in digital steganographic applications such as for secret transactions in an inconspicuous manner. The survey for the proportion of cover objects used in digital steganographic applications done by Johnson & Sallee (2008) (shown in Figure 1.1) also supports it.
Let $C$ denote the set of all cover images and $M$ be the set of all message signals. Let $K$ be the set of all keys and $C'$ be the set of all modified cover images. The embedding method is a method for embedding a message signal in a cover image. According to Chvarkova et al. (2011), we define the embedding method, $E$ by the mapping

$$E: C \times M \times K \rightarrow C' \text{ such that } c^* = E(c, m, k) \text{ for all } c \in C, m \in M, k \in K$$

Here, $c^* \in C'$ is the modified cover image. The modified cover image after embedding is also called a stego-image. The redundant space of the cover image which is available for steganographic modification and message signal transmission is called the Steganographic Channel space, $SC$. The extraction method is the method of decoding of the modified cover image in order to get the message signal, $m$. It is defined by the mapping

$$D: C' \times K \rightarrow M \text{ such that } m = D(c^*, k).$$

The set of coding and decoding methods executed with steganographic objects, applying the restriction on steganographic channel space, is called the Steganographic System, SS.

Mathematically we define SS as the pair $<SSE_{sc}, SSD_{sc}>$, where $SSE_{sc}$: $C \times M \times K \rightarrow C'$ is defined by

$$SSE_{sc} (c, m, k) = c^* \text{ for all } c \in SC, m \in M, k \in K$$
and \( SSD_{sc} : C' \times K \rightarrow M \) is defined by

\[
SSD_{sc}(c^*, k) = m
\]

**Figure 1.2: General model for steganographic system**

The Figure 1.2 depicts a general model of stego system which includes compression techniques, cryptography and ECCs. The modern image steganographic process thus consists of the following steps:

1. The selection of cover image or its portions that is/are made available for modification (SC).
2. Compressing the original message and/or encoding with the encryption technique or ECCs technique or both to obtain the secret message.
3. Embedding the secret message in the cover image, “c” via steganographic method, \( E \) using a unique key ‘\( k \)’ that is known to sender and receiver only.
4. Decoding the secret message obtained from stego-image using the extraction method and the unique key, ‘\( k \)’ at the decoder end by recipient.

The stego-object should satisfy all steganographic requirements such as the size stego-object should be a same as of the cover-object and it should be without any perceptual distortion of the host signal so that it cannot be distinguished from over image, “c”. Else the eavesdropper can try to attack the stego, try to decode the secret message in the
Chapter 1

attack channel, if suspected. Further, the distributions of the cover image “c” and the modified image, “c*” must also be same for the security against statistical attacks.

1.1.1. Attributes of steganography

The basic attributes of steganography are *imperceptibility (invisibility), capacity (payload), security, undetectability and robustness* against statistical attacks or common-carrier attacks (Zaidoon et al., 2010). According to Cox (2009), robustness should not be considered as an attribute of steganography as it is then difficult to differentiate it from watermarking.

To provide an additional layer of security, Cryptography, Compression and Error Correction Codes methods have also been used in conjunction with Steganography. These techniques are independent of an image formats and hide data in more significant areas of the transformed image (Zielinska et al., 2012).

The characteristics of steganography alongwith the metrics for each are shown in Figure 1.3. For measuring *imperceptibility*, most of the researchers have come to conclusion that PSNR or WPSNR can be used to measure the quality of image after embedding. Another metric, SSIM, is used for measuring the structural similarity between images. It is designed to improve on PSNR which has proven to be inconsistent with human eye perception (en.wikipedia.org/wiki/StructuralSimilarity). By Security we mean cryptographic security which should make the scheme so hard that adversary cannot break it. The *security* of the technique can be guaranteed using keys at encryption/ compression stage. One can also use pseudo-random keys while embedding the secret message in the cover image. The *robustness* is usually required against the noise of communication channel while the stego-image is transmitted to receiver through it. Also to find whether the method has provable security from the eavesdroppers, the measure KLDiv is used for stego-image as suggested by Cachin (1998). If its value is zero, it shows that the technique is provably secured.

Apart from the secure communication, Steganalysis (the art of detecting the existence of hidden information) is another important concept in a steganographic system (Chanu et al., 2012). It attempts to defeat the goal of steganography. There are number of Steganalytic tools (Hayati et al., 2011) that can be used to detect hidden data in the
suspected image. Steganalysis has its applications in cyber warfare, computer forensics, tracking criminal activities over the Internet and so on. It is also practiced for evaluating, identifying the weakness and improving the security of steganographic systems.

Figure 1.3: Attributes and corresponding metrics of Steganography. The level of metrics may be specified in any order.

Though visual imperceptibility is the first requirement of any steganography system, but it is no longer sufficient as the statistical attacks have been applied by steganalyst to reveal the traces of embedding. Modern steganalysis techniques classify images based on changes and boundaries in statistics across an image rather than any visual artefacts (Fridrich & Goljan, 2002). Thus, for some researchers (Kodovsky and Fridrich, 2008), the main requirement of steganography is Undetectability. One should not be mistaken for imperceptibility which is a concept related to human perception with undetectability. Undetectability means the impossibility to prove the presence of a hidden message. Detectability refers to the extent to which steganalysis techniques detect stego-images through statistical means. A system that is undetectable will also be imperceptible but the opposite is not true. The ability to detect the presence does not automatically imply the ability to read the hidden message. To meet this requirement, Shin (2006) has suggested two defending approaches, viz., Pseudo-Random Number Generator, i.e., using the keyed PRNG to select the redundant data and Error Correction Codes that allow us to use the unmarked redundant data bits.
There are studies on detection techniques (Westfeld, 1999; Farid, 2002; Zhang, 2003; Fridrich et al., 2001), most of which analyze the pixel value distribution on a suspicious image for detecting the hidden message. One of such method for detection is based on difference image histogram (Zhang, 2003). Solanki et al. (2006) have proposed zero K-L divergence between the cover and the stego-signal distribution as the provable security for the design of embedding scheme that can evade statistical steganalysis while hiding at high rates and achieve robustness against attacks.

1.1.2. Classification of steganography schemes

Depending on the applications, Steganography schemes have been classified in many ways which are summarized as follows (also see Figure 1.4):

I. According to the written quomodo (cover file), these schemes are divided into Spatial (Image) Domain information hiding and Frequency (Transform) Domain information hiding by Kharrazi (2004). Most spatial domain methods, e.g., LSB have zero error rates (Bruen & Forcinito, 2005). But, when the hiding is done in transform domain (e.g., wavelet domain and Fourier domain), some errors are introduced (Cheddad et al., 2010). There are Error Correction Coding methods, which can be used to achieve zero error rates (Hamming, 1950; Mcwilliams, 1977). There has been a vast research in the recent years in the spatial and transform domains for finding a high quality, high payload, secure and robust steganography scheme. The schemes in the spatial domain still have relatively low-bit capacity and are not resistant enough to lossy image compression and other image processing. On the other hand, frequency domain-based techniques can embed more payload and are more robust to attack.

II. According to Payload, the steganography schemes are classified into High bit-rate data hiding and Low bit-rate data hiding (Tolba & Ghonemy, 2004). By bit-rate, we mean the amount of data that can be embedded as a portion of the size of the cover image. It is well known that high bit-rate data embedding usually have impact upon the perceptibility of the cover-object. Therefore, to design a high bit-rate steganography method, it is important that such impacts are minimized. Moreover, to make such methods to be robust against statistical or image carrier attacks, error correction codes may be used.
III. According to the confidentiality, Chou (2012) has divided the steganography schemes into Distortion-free or Reversible steganography and Fragile or Irreversible steganography. Reversible methods are those that allow embedding data inside an image and later not only the hidden data can be retrieved but the exact copy of original image can also be recovered. In the irreversible methods it is not desirable to recover the original image after the hidden data is retrieved.

IV. According to Protection, Reddy et al. (2012) have classify them into Protection against detection (i.e., data hiding) and Protection against removal (Watermarking and fingerprinting)

V. According to the structure of the classification system, Katzeneisser et al, (2000) have divided the steganography technique into three types: Pure Steganography, the Secret Steganography and the Public Key Steganography. The pure steganographic system does not require the prior exchange of some secret information (like a stego-key), thus the security of the system depends entirely on its secrecy. In the secret key steganography system, the sender choses a cover and embeds the secret message into the cover using a secret key (e.g., a stego-key), which is shared by receiver. Since the stego-key is not known to anyone else, any eavesdropper should not be able to obtain evidence of the encoded information. In the public key steganography system which is proposed by Anderson et al (1998), embedding is done using the public key of the receiver and extraction is done by the receiver using its private key.

VI. According to the carriers, it also can be divided into Text information hiding, Image information hiding, Audio information hiding, Video information hiding and so on (Alanazi, 2010).

1.1.3. An overview to transforms

There are large number of transforms available, both discrete and continuous. Having assessed the most used transforms in that list, this thesis presents with the best suited steganography algorithms for each transforms, as well as the alternatives such as error correcting code based steganography that are available for it. Some transforms such as Discrete Fourier transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Discrete Contourlet Transform (CTT), Singular Value
Decomposition (SVD) Transform and Discrete Hadamard Transform (DHT) are used by researchers for steganography in the frequency domain.

Apart from using DFT and DCT, the problem of selecting a suitable wavelet transform for signal and image processing has always challenged the researchers. For image steganography, the researchers have used mainly Integer Wavelet Transforms, viz., Haar Wavelet or CDF (2, 2). There are research papers investigating different wavelet transforms and finding a suitable wavelet for image compression or image denoising, but the research on investigating wavelet transforms for the steganography is still an open problem. In image compression/signal processing, wavelet transforms are most widely-used tool due to its inherent multi-resolution representation akin to the operation of the human visual system. They reduce blocking artifacts to a great extent than the DCT and provide higher compression ratio. They are adopted in JPEG2000. They also perform well in image de-noising. However, 2D wavelet transform is, intrinsically, a tensor-product implementation of the 1D wavelet transform and it provides local frequency representation of image regions over a range of spatial scales and it does not represent 2D singularities effectively. Therefore, it does not work well in retaining the directional edge in the image and it is not sufficient in representing the contours not horizontally or vertically, i.e., they lack directional selectivity for diagonal features and shift invariance. There are two deviations from wavelets to find a solution of these problems. One direction is towards Curvelets and another direction is towards CWTs.
The Contourlet transform (CTT), introduced by Do and Vetterli (2005), is a true 2-D geometrical image based transform. It overcomes the difficulty in exploring the geometry in digital images due to the discrete nature of the image data. It possesses the important properties of directionality and anisotropy which wavelet does not possesses. It can represent a smooth contour with fewer coefficients compared to wavelets. They have the properties such as Multiresolution (representing images from a coarse level to fine-resolution level), Localization (Basis elements can be localized in both the spatial and the frequency domains), Critical sampling (representation form a basis, or a frame with small redundancy), Directionality (representation of basis elements oriented at variety of directions) and Anisotropy (capturing of smooth contours in images). The first three properties are also provided by separable wavelets. However, CTT is not shift invariant. A new derivative of CTT called Non-subsampled Contourlet Transform (NSCT) was proposed by Cunha, Zhou and Do (2005). The NSCT is obtained by coupling a nonsubsampled pyramid structure with the nonsubsampled DFB. Navas et al (2009) have proposed a novel blind reversible data hiding algorithm for telemedicine applications using NSCT. The method proposed by them has the advantages of high capacity, imperceptibility and robustness to attacks.

Kingsbury (2000) and Selesnick et al. (2005), both introduced Dual-Tree Complex Wavelet Transform (DT-CWT). Selesnick (2001-2004) also provided Double-Density DWT (DD DWT) and Dual-Tree DWT (DT DWT) for complex analysis. They have shown that DT-CWT has a modest amount of redundancy, but it provides shift invariance and good directional selectivity. However, the research on applying the wavelets to data hiding techniques is still too limited, only a few publications deal with this topic at present. More details about these transforms can be found in the introduction of chapters 3 to 7 in this thesis.

1.2. PROBLEM EVOLUTION

It is not possible to maximize imperceptibility and capacity and improve robustness, simultaneously in any data hiding scheme. Therefore, the acceptable balance of these parameters must be struck based on the particular application/goal. For example, a steganographic scheme may forgo robustness in favour of capacity and low
perceptibility, whereas a watermarking scheme, which may not require large capacity or low perceptibility, would certainly support increased robustness. According to Marvel (1998), steganography used as a method of secret communication would adopt the utmost imperceptiveness while sacrificing robustness and possibly capacity.

![Figure 1.5: Trade-off among security, robustness, undetectability, transparency and payload (Cacciaguerra & Ferretti (2000) and Fridrich (1998))](image)

Figure 1.5 depicts the relationship between the characteristics of steganography. It shows that if we want to embed high payload then, either transparency may be lost or the stego-system may not remain robust to common statistical attacks or the message may become detectable by the eavesdropper.

In most of the steganographic methods, the data embedding process consists of mainly three steps:

**Step 1.** *Encoding the message by some appropriate codes to convert the data into a bit pattern*

**Step 2.** *To determine the redundant bits/pixels in the cover or its transformed image that can be modified so that the image quality is not degraded.*

**Step 3.** *Embedding the secret data bit stream into the selected redundant coefficients of cover image or into the subbands obtained by applying transformation to cover image, thus creating the stego-image.*

According to Fridrich, Goljan & Sonkal (2006), Schonfield & Winker (2007) and Munuera (2007) remarks, the four main goals of the design of good steganographic algorithms that makes the data hiding secure are:
(i) *The choice of proper covers,*

(ii) *The search for techniques for embedding message in the cover in an imperceptible way.*

(iii) *To modify the cover data as little as possible to make it robust from the accidental distortion (i.e., against common statistical and image-carrier attacks) and*

(iv) *Compressing the message/apply encryption before hiding in the cover.*

Thus, the problems in a steganographic scheme can be summarized as follows:

1. *Modification of the cover-object when the message is embedded in it.* It is well known fact that distortion in the cover object happen when the data payload is increased during the embedding process. Thus, it is the first requirement of data hiding that distortions in the cover object be minimized

2. *The search for the suitable technique for embedding.* There are various features such as Payload, Perceptual transparency, Robustness, Undetectability and Computational complexity which characterizes the strength and weakness of a steganographic technique. Further, not all steganographic methods are suitable for a particular application. The suitability of a method depends on number of factors such as the type of data, the processing or transformations applied on data, the lossy or lossless type of compressions used, the key type used, etc. An objective and quantitative measurement on the suitability of each method for a given application is of great importance and usefulness.

3. *Robustness to common statistically and cover-carrier attack.* There are applications that require the data hiding schemes to be non-fragile or robust, that is, hidden Message should be extracted successfully even when the slightest alteration has been made to the marked image. Katzenbeisser, Fabien, Petitcolas (2000), have mentioned that robustness is a practical requirement for a steganography system. It is required to create an undetectable steganographic algorithm that is capable of resisting common image processing manipulations that might occur accidentally and not necessarily via an attack. The most common noise introduced during image processing is Gaussian noise (Lou, Hu and Liu, 2002).
4. **High embedding capacity.** The steganography, strictly speaking, focuses in transmitting high amounts of information in an imperceptible manner, although less robust. The amount of hidden information that can be hidden compared to the amount of carrier information, always without breaking any other requirement (invisibility, robustness etc. (Rico, 2010)).

5. **Undetectability vs Invisibility.** For some researchers (Kodovsky & Fridrich, 2008), the main requirement of steganography is Undetectability. However, it should not be mistaken it with invisibility (a concept related to human perception). Undetectability means the impossibility to prove the presence of a hidden message. This concept is inherently tied to the statistical model of the carrier image. The ability to detect the presence does not automatically imply the ability to read the hidden message. To meet this requirement Shin (2006) has suggested two defending approaches, viz., *Pseudo-Random Number Generator* and *Error Correcting Codes* which allows using the unmarked redundant data bits.

6. **Complexity and computational cost.** Normally, in steganography techniques, the complexity, depends on the context, is not a very important characteristics. In fact, if the transmission does not take place in real time, the sender can use as much time as needed, so this requirement will not be so important (Rico, 2010).

7. **The loss of synchronization at decoding stage.** Many compression schemes make use of variable length codes (VLCs) for entropy encoding as they are very efficient in reducing the bit-rate but they have a disadvantage of losing synchronization at the decoder when an error occurs.

Manoharan (2003) proposed the use of T-codes to encode messages prior to embedding the messages in the cover media. The extracted messages need to be decoded before use. According to him, this system will be more tolerant to media transformations that result in some bit losses or bit inversions in the hidden message. A steganography system using T-codes given by him is shown in Figure 1.6.
1.3. RESEARCH TOPIC

Keeping in mind the requirements of high imperceptibility of stego-image, high embedding capacity and undetectability of steganography scheme, we embark upon the task of investigating wavelet-like transforms and complex wavelet transforms for their inherent properties in steganography. The emphasis of current research has been focused more towards searching of best transform or an alternative technique in the design of image steganographic method than developing novel hiding methods. Researchers in the field of digital communication have long used Huffman codes as source encoding, but in the field of steganography, it appears, the self-synchronizing concept has not been touched much. Thus, irrespective of the data hiding technique followed the role of SSVLC, viz., T-codes in steganography in the context of source encoding and self-synchronization is investigated. Finally, for the requirement of robustness, Advanced Encryption Technique (AES) and Error Correcting Codes (ECC’s), viz., Reed-Muller codes and Reed-Solomon codes over Hamming codes would be investigated. The proposed topics are:

1. *Investigation of Wavelets, Wavelet-like transforms, Directional Transform (Contourlet) and Complex Wavelet transforms for designing a secure and high capacity steganography scheme*
2. Role of Self-synchronizing variable length codes (T-codes) in reducing the probability errors at decoding stage and achieving robustness and

3. Role of Error Correcting codes (Hamming, Reed-Muller and Reed-Solomon) in designing image steganography scheme with efficient embedding efficiency and achieving high embedding capacity and robustness.

Further, for steganalysis, it is proposed to study

(i) the pixel histogram analysis between the test cover-images and the stego-images generated by different schemes to observe the security of the data hiding methods and

(ii) the K-L divergence values for the stego-images with respect to the embedding capacity

Thus to summarize in brief, image steganography algorithms based on the following different schemes given below are presented:

(i) Irreversible schemes in grayscale image using Modified (or randomized) LSB and LSB varying mode,

(ii) Irreversible schemes in color image using Fusion technique and

(iii) Reversible scheme in grayscale image using thresholding technique.

Modified LSB technique is simple, fast, high capacity method, however, not found to be robust against common statistical attacks. LSB varying mode method is a high capacity image steganography proposed by Chen and Lin (2006) in the Haar Wavelet transform that provides better PSNR with respectable security. This method has weakness that it needs extra information, key matrix, to be sent along with the stego-image to the receiver. Wavelet Fusion method is another high embedding steganography technique for color image proposed by Tolba and Ghonemy (2004). Their method provides the high invisibility as well as the large hiding capacity. The reversible thresholding technique is a Companding technique suggested by Xuan, Shi, Yang, Zhang, Zou and Chai (2002). These techniques are required for the applications such as medical, astronomical, law enforcement and others. We summarize the above techniques in the next subsection.
1.4. REVIEW OF STEGANOGRAPHIC SCHEMES

Although steganography for binary images and 2-D images have some progresses, researches mainly concentrate on hiding data in grayscale images and color images. It is generally considered that grayscale images are more suitable than color images for hiding data because the disturbance of correlations between color components may easily reveal the trace of embedding. But the steganographic using color images has attracted researches as the color image provides three times embedding capacity than the grayscale image. So, we shall focus on both these schemes of steganography in the thesis. For grayscale images, the steganography schemes used are Modified LSB fixed Mode, Modified Varying Mode and Reversible Companding technique. For color image based steganography we have evaluated Wavelet Fusion method based on different transforms. We review the steganographic schemes in this section whose performance is evaluated using different transforms and error correction codes.

1.4.1. Modified LSB fixed mode (MLSB-FM) technique

The least-significant bit (LSB) insertion method is the most common method for embedding messages in an image. The basic idea of LSB embedding is to embed the message bit, \( b \), at the rightmost bits of pixel value, \( x \) so that the embedding method does not affect the original pixel value greatly. The formula for the embedding is as follows:

\[
x' = x - x \mod 2^k + b
\]

where \( k \) is the number of LSBs to be substituted.

The extraction of message from the high frequency coefficients is given as:

\[
b = x \mod 2^k
\]

There are two types of LSB insertion methods, fixed-sized and variable-sized. The former embeds the same number of message bits in each pixel of the cover-image. On embedding fixed four random bits in the four LSBs of each pixel, some false contours can occur. The unwanted artifacts may raise suspicion and defeat the purpose of steganography. To treat this problem, either fewer bits must be used for message embedding or a variable-sized method needs to be applied. For the variable-sized
embedding method, the number of LSBs in each pixel used for message embedding depends on the contrast and luminance characteristics. Thus the most important requirement is maintaining the image fidelity while adapting these local characteristics to estimate the maximum embedding capacity (Chin and Lin, 2006).

The modified (or randomized) LSB (MLSB) technique uses a randomized permutation function to permute the coefficients of detail sub-bands obtained from the cover image before embedding the secret message using LSB technique. This technique, however, is still vulnerable to replacing the LSB’s with a constant but it proves to be a simple and fairly powerful tool for steganography at the expense of its low fidelity in secret communications. In case one expects no intentional attacks, for sake of its simplicity, the MLSB technique for data hiding can be used.

1.4.2. MLSB varying mode (MLSB-VM) technique

Chen and Lin (2006) have proposed LSB based image steganography techniques in wavelet domain. The embedding procedure is classified into two modes: Varying mode and Fix mode. In Fixed Mode, there is a specific range for required capacity whereas in varying mode the range of capacity is not specific and differs. In the varying mode case, first every 2 consecutive bits of binary string are combined to form a decimal value from 0 to 3. Every 2 consecutive values in the resulted decimal sequence are further combined to perform subtraction operation and form a differential sequence ranging from -3 to 3. The four possible absolute values (0, 1, 2 and 3) are embedded in sub-band HH by substituting 2 LSBs of coefficients of HH with 00, 01, 10 and 11 respectively. The Subtraction pairs, embedding is done in LH and HL sub-bands. The remaining bits of message are embedded at those unused LSBs in LH and then HL bit by bit. Since after embedding and taking the inverse DWT, some pixels in stego-image are not integers, we record the 4 possible non-integer situations (0.0, 0.25, 0.5 and 0.75) in the key-matrix, K. This matrix is required to perfectly reconstruct the secret message bits in the extracting procedure. Chen and Lin (2006) have observed after the implementation of other algorithms on different images that the PSNR is a satisfactory value even when the highest capacity case is applied and Key-matrix provides an additional layer of security.
1.4.3. Reversible companding method

The companding is the process of signal compression and expansion. The compression function, C maps large range of original signals x, into narrower range, \( y = C(x) \) whereas expansion, E is the reverse process of compression, \( x = E(y) \). After expansion, the expanded signals are close to the original ones. Assume the original signals are x. If the equation \( E[C(x)] = x \) is satisfied, then this kind of companding could be applied into reversible data hiding.

Let \( y = C(x) \), \( y = y_1y_2y_3...y_n \), \( y_i \in \{0, 1\} \).

Let \( t \in \{0, 1\} \), \( y' = y_1y_2y_3...y_n t \), then

\[
y' = P(y) = 2^y \text{(shift left y)} + t,
\]

where \( t \) is the hiding data. If \( y' \approx x \), modification of signal will hardly be perceived. By hiding data extraction process, extract LSB of \( y' \), i.e. \( t = \text{LSB (} y' \text{)} \) and recover signal \( y = (y' - t)/2 \). Finally, recover original signal x by expansion \( x = E(y) \).

So, two conditions must be satisfied:

1. Since, \( y = C(x) \), \( x = E[y] \), \( \Rightarrow E[C(x)] = x \); Thus the first condition is: \( E[C(x)] = x \);
2. Also, \( y' = P(y) = 2^y + t \approx x \), \( \Rightarrow P[C(x)] \approx x \); therefore the second condition is: \( P[C(x)] \approx x \).

For the first condition, any one-to-one mapping function can be used. For multiple \( x \) mapped to single \( y \), still could be used, e.g., if \( x_0, x_1 \rightarrow y \), then use bit “0” to indicate \( x_0 \) and bit “1” to indicate \( x_1 \). These overhead data also need to be embedded into original signal. So, the first condition is easy to be satisfied.

For the second condition, based on the study of Human Visual System (HVS), it is noted that slight modification on wavelet high frequency subband, HH coefficients is hard to be perceived by human eyes. Since the method to compand image is to slightly change wavelet high frequency sub band coefficients for hiding data, so the second condition could be satisfied.

A reversible companding method for the lossless data hiding is given by Xuan et al. (2002). In this method a threshold value is predefined. To embed data into a high
frequency coefficient of sub-band HH, LH or HL, the absolute value of the coefficient is compared with T. If the absolute value is less than the threshold, the coefficient is doubles and message bit is added to the LSB. No message bit is embedded otherwise; however, the coefficients are modified as follows:

$$x' = \begin{cases} 
2^*x + b & \text{if } |x| < T \\
x + T & \text{if } x \geq T \\
x - (T - 1) & \text{if } x \leq -T 
\end{cases}$$

where T is the threshold value, b is the message bit, x is the high frequency coefficient and x' is the corresponding modified frequency coefficients.

To recover the original image, each high frequency coefficient can be restored to its original value by applying the following formula:

$$x = \begin{cases} 
L x'/2 & \text{if } -2T < |x'| < 2T \\
x' - T & \text{if } x' \geq 2T \\
x' + T - 1 & \text{if } x' \leq -2T + 1 
\end{cases}$$

The Figure 1.7 provides an example to hide the message, s=011010 into a block of 3x3 where T=10. In the next subsection we now discuss a high bit rate irreversible data hiding technique for color images.

1.4.4. Wavelet fusion method

The Wavelet fusion method is the High bit rate data hiding. In this method the fusion process takes place between the DWT of the secret data and the DWT of the cover...
image. Since the ordinary wavelet filters have floating point coefficients, a normalization operation is applied on the cover image so that the wavelet coefficients are converted in the range of 0.0 and 1.0. The fusion technique then merges the wavelet decomposition of both the cover image and the secret message into a single fused result using the following equation:

$$f^*(x, y) = f(x, y) + \alpha g(x_m, y_m)$$

where $f^*$ is the modified DWT coefficient, $f$ is the normalised wavelet coefficient, $g$ is the normalized message coefficient and alpha ($\alpha$) is the embedding strength which ranges from 0.0 to 1.0. To overcome the problem of overflow or underflow, the cover’s normalized pixels are adjusted before the embedding process takes place so that the reconstructed pixels do not go out of range. The secret message is converted to binary bits and if the bit is 1 the $+\alpha$ is added to the cover image wavelet coefficient and if it is 0 the $-\alpha$ is added to the wavelet coefficient of the cover image. The embedding is applied on each color plane separately. Tolba, Ghonemy, Taha & Khalifa (2004) have proposed this method where the secret data is another color image.

### 1.4.5. Matrix encoding

Matrix encoding is an interesting error correction codes based steganographic method which was introduced by Crandall (1998). Matrix encoding requires the sender and the recipient to agree in advance on a parity check matrix $H$ and the secret message is then extracted by the recipient as the syndrome (with respect to $H$) of the received cover object.

The matrix encoding technique is summarized by Fridrich and Soukal (2006) as follows:

**Algo 1.4.5.1: Matrix Encoding**

```
Input: A vector of bits $x \in GF(q^n)$ from the cover objects (e.g. LSBs of a subset of pixels), $H$, a parity check matrix of dimension, $(n-k) \times m$ is the message

Output: Stego-vector, $y$
```
Step 1. Read $n$-bits (denoted by $x$) from the cover object and $(n-k)$-bits message

Step 2. Calculate the syndrome $Hx$.

Step 3. Find any $e$ that solves the equation: $He = m - Hx$.

Step 4. In the list of all $2k$-codewords, $e$ is coset leader of the family of cosets, $C(m - Hx)$.

Step 5. Modify the cover, $y = x - e$.

Step 6. $y$ is the final vector containing message.

The message bits are extracted following the same path as followed in embedding and calculating $(n-k)$-bits from each segment of $n$-bits $y$ of the stego object by

$$Hy = Hx + He = Hx + (m - Hx) = m$$

Here, $m$ is the extracted message.

1.4.6. Hamming based error map technique

With the encoding redundancy of Error-Correcting codes a new steganography method is proposed by Liu et al (2006) (Figure 1.8(a)). A mapping code between secret information and codeword error map is built as shown in Figure 1.8(b). By modifying the part of the codeword of the error-correcting codes according to the error map secret information is embedded. This method can be used with different codes.
For example, suppose we wish to send $c = (100000000000011)$ with the secret message 110. Then by changing $c$ to $r = (100000001000011)$ using the error map, secret message is embedded. Now, on receiving $r$, we calculate $s = rH^T = 1001$. The secret message 110 then could be obtained using error map.

1.4.7. Pre-flipping algorithm in hamming codes

Schonfeld and Winkler (2007) have proposed a method to improve embedding efficiency. In this approach, the parity check matrix has a special structure $H_{k \times n}$, corresponding to a systematic code, $[a_l, a_k]$ where $a_l$ covers the $l$ information bits and $a_k$ covers the $k$ parity bits. In the basic embedding process, the syndrome $s$ of length is calculated as $s = \text{mod} (a, g)$, where $a$ is codeword and $g$ is generator polynomial. To embed $emb$ into $a$, $s$ is combined with $emb$ using XOR operation. According to authors, we can improve embedding efficiency by considering a $a_l$, i.e., we do not flip only bits within the $k$ parity bits, but also one information bit within $a_l$. The heuristic approach needs $l$ pre-calculation steps. In each step $i$, ($i = 1, 2... l$), we pre-flip one out of the $l$ information bits in $a_l$ and determine the syndrome $s$ as $s_i$ as described: The weight of $(s_i \Theta emb)$ is found in order to find the combination with minimal Hamming weight. The total number of bits that have to be flipped (including the pre-flipped bit) is now $w_1 = \min_{i=1} (w(s_i \Theta emb) + 1)$. Whenever, $w_1$ is smaller than $w_2 = w (s_i \Theta emb)$, calculated with the original unmodified $a_l$), we flip the $w_1$ bits. Otherwise we flip $w_2$ bits of the $k$ parity bits. The authors have shown in the paper that as a result of this heuristic approach, the embedding efficiency can considerably be increased.
1.5. PERFORMANCE MEASURES

The performance of the proposed techniques given in the thesis is evaluated according to the widely used metrics: PSNR, SSIM and KLDiv and Embedding efficiency.

1.5.1. Imperceptibility

This aspect measures how much difference (distortion) was caused by data hiding in the original cover, where the higher the stego-image quality, the more invisible the hidden message. We can judge the stego-image quality by using Peak Signal to Noise Ratio (PSNR). The PSNR for an image of size N x N is given as follows:

\[
PSNR = 10 \log_{10} \left( \frac{c_{\text{max}}^2}{MSE} \right) \text{ (dB)},
\]

\[
MSE = \frac{1}{N^2} \sum \sum (x_{ij} - x'_{ij})^2,
\]

where \( c_{\text{max}} = \begin{cases} 
1 & \text{in normalized double precision range} \\
255 & \text{in 8-bit unsigned integer values} 
\end{cases} \)

The MSE is the Mean Square Error, \( x_{ij} \) stands for the image pixel value in the cover image and \( x'_{ij} \) is for the pixel value at position \((i, j)\), in the image after inserting secret message. A high value of PSNR means better image quality (less distortion), it is recorded that in grayscale images that the human visual system (HVS) can’t detect any distortions in stego-images having PSNR that goes beyond 36 dB. Navas et al. (2009) have used WPSNR (Weighted Peak signal to Noise Ratio) to determine the degradation in the embedded image with respect to the original image. WPSNR takes into account the texture of the image, based on the fact that the human eye is less sensitive to changes in textured areas than the smooth areas. It is defined as

\[
WPSNR = 10 \log_{10} \left( \frac{c_{\text{max}}^2}{MSE \ast NVF} \right) \text{ (dB)}
\]

\[
NVF = \text{NORM} \left\{ \frac{1}{1 + \delta^2} \right\},
\]

Here, \( \delta \) is the luminance variance for the 8 x 8 blocks of the image and NORM is the normalization function. NVF uses a Gaussian model to estimate the amount if texture content in any part of the image. In the regions with edges and texture, NVF will be greater than 0 while in smooth regions it will be closer to 1.
1.5.2. PSNR for color images

There exist different approaches for computing the PSNR of a color image. According to Mathworks (http://www.mathworks.in/help/vision/ref/psnr.html), the PSNR for color images can be computed by first converting the image to a color space that separates the intensity (luma) channel, such as YC\(_b\)C\(_r\), and then the PSNR can be obtained only on the luma channel, (denoted by PSNR\(_Y\)). The recommendation for this approach is suggested because the human eye is most sensitive to luma information, the Y (luma), in YC\(_b\)C\(_r\) represents a weighted average of R, G and B and G is given the most weight, again because the human eye perceives it most easily.

Alternately, for color images with three RGB values per pixel, the definition of PSNR is the same as for a noise free (m x n) monochrome image, except the MSE is the sum over all squared value differences divided by image size and by three (http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio). This is denoted as PSNR\(_E\) in the thesis.

Recently, Yalman and Erturk (2013) have proposed a simple and effective full-reference color image quality measure (CQM) based on reversible luminance and chrominance (YUV) color transformation and peak signal-to-noise ratio (PSNR) measure. The CQM value is given as:

\[
CQM = (PSNR_Y \times R_W) + \left( \frac{PSNR_U + PSNR_V}{2} \right) \times C_W,
\]

where the CQM is composed of the weighted luminance quality measure (PSNR\(_Y\)×R\(_W\)) and weighted color quality measure (PSNR\(_U\) + PSNR\(_V\)) ×C\(_W\)) components. C\(_W\) is the weight on the human perception of the cones and R\(_W\), is the weight on the human perception of the rods. The values of C\(_W\) and R\(_W\) are calculated as 0.0551 and 0.9449, respectively. The notation PSNR used for color images will mean the average value of PSNR calculated for each of the Red, Green and Blue channels.

1.5.3. Structural similarity index measure (SSIM)

The mean similarity measure was proposed by Wang et al. (2004) to evaluate the quality of stego-image, F with respect to the original image, E, given by
\[
SSIM (E, F) = \frac{(\mu_{x} \cdot \mu_{y} + C_{1}) \cdot (2\sigma_{xy} + C_{2})}{(\mu_{x}^2 + \mu_{y}^2 + C_{1}) \cdot (\sigma_{x}^2 + \sigma_{y}^2 + C_{2})}
\]

where \(\mu_{x}, \mu_{y}, \sigma_{x}, \sigma_{y}\) and \(\sigma_{xy}\) local statistics parameters of the two images \(E\) and \(F\) and \(C_{1}, C_{2}\) are constants used to make it finite.

The SSIM index models any distortion as a combination of three different factors: loss of correlation, luminance distortion and contrast distortion. The mean similarity measure MSSIM varies in the interval \([-1, 1]\). The best value 1 is achieved if and only if \(E=F\).

### 1.5.4. Kullback-Leibler divergence (K-L divergence)

According to Cachin (1998), a steganography algorithm is \(\varepsilon\)-secure if the relative entropy (also called K-L divergence) between distributions of cover object and stego-object is less than or equal to \(\varepsilon\). For the design of embedding schemes that can evade statistical steganalysis while hiding at high rates and achieve robustness against attacks, zero K-L divergence between the cover and the stego signal distributions is proposed by Solanki et al. (2006) as the provable security. K. L. divergence is a measure of distance between two probability distributions.

Let random variable \(C\) and \(S\) denote the cover image and stego image respectively and let \(P_{C}\) and \(P_{S}\) represent the probability mass functions (pmfs) of \(C\) and \(S\), respectively. The K-L divergence between these two pmfs, \(P_{C}\) and \(P_{S}\), is defined as:

\[
D (P_{C} || P_{S}) = \sum_{g \in G} P_{C}(g) \log \left( \frac{P_{C}(g)}{P_{S}(g)} \right)
\]

where \(g \in G \approx \{0, 1, 2, ..., 255\}\) is the pixel value in grayscale images.

The stego system is considered perfectly secure in the Cachin’s sense if \(D (P_{C} || P_{S}) = 0\). It is called \(\varepsilon\) -secure, if \(D (P_{C} || P_{S}) \leq \varepsilon\). It is proved that there exists a perfectly secure steganographic system (Katzenbeisser et al (2000)).

### 1.5.5. Embedding efficiency

Let \(R_{a}\) be the average number of embedding changes. For the stego-codes, \(SC (R_{a}, N, n)\) which can embed \(n\) bits of message bits in \(N\) pixels with at most \(R_{a}\) modifications, we define
(i) the embedding rate by $\alpha = n/N$, which is the number of bits carried by each pixel;
(ii) the average distortion by $D = Ra/N$, which is the average changing rate of the cover image and
(iii) the embedding efficiency by $e = n/Ra = \alpha/D$, which is the average number of embedded bits per change.

1.6. ORGANIZATION OF THESIS

The Figure 1.9 highlights the classification of research work in image data hiding using steganography into different chapters.

The current Chapter 1 is introductory one.

In Chapter 2, Steganographic algorithms based on distinct error correction codes are presented. First, an image steganographic algorithm based on RM-codes and RS-codes
using error map method is proposed. A comparative analysis of proposed algorithm is done with Hamming based classical Matrix Encoding and Hamming based error map method given by Quing et al (2006). The experimental results show that the proposed algorithms have better imperceptibility, multi-layered security, provable security and constant embedding efficiency.

Next, a robust and secure image steganography in which two pre-processing steps are used before the embedding algorithms is proposed. In the beginning a self-synchronizing T-codes are used to generate compressed encoded data stream. Then, for the purpose of increasing the image Steganography robustness against attacks of an image transmission, the compressed encoded data stream is encrypted with RS-codes. The data stream so obtained becomes robust and secure for hiding in the bit-planes of the cover image. The selection of the bit-plane for embedding is determined based on its complexity. If the complexity of region is greater or equal to a threshold value, we deem that bit plane is embeddable and if not, we leave that bit-plane alone. The threshold value is defined as a function of mean and variance values of the bit-planes. The proposed method is compared with other methods such as simple syndrome embedding, improved pre-flipping method and error map technique based on Hamming codes. Experimental results show that the proposed method is improvement over the existing methods.

In Chapter 3, High capacity image steganographic algorithm based on DCT is studied. The algorithm is based on Jpeg-Jsteg and OutGuess 0.1 methods in which Huffman codes are replaced by T-codes. First a single bit embedding is done and experimental results show that T-codes improve the results in terms of better PSNR. Next, the message is embedded using 4-bit XOR-operation in the randomized and quantized middle frequency coefficients of DCT. The T-codes are used as source encoding for obtaining secret message as well as in entropy encoding for obtaining the stego-image. Through implementation of algorithm on different image formats, it is observed that the image quality of image, in terms of PSNR, remains linear at the reasonable value even when the message capacity increases. Thus the proposed high capacity Algo 3.3.1 not only provides better embedding capacity, but also reasonable image quality.
In Chapter 4, Image Steganographic schemes are extended to Discrete Wavelet Transforms. In the beginning of the chapter we analyze different orthogonal wavelet filters using the randomized LSB method. It is observed through the experimental results that the performance of Haar wavelet is much better than the other wavelets in terms of perceptibility and security. Another algorithm is discussed to evaluate the performances of Haar wavelet and biorthogonal CDF9/7 wavelet in image steganography. It is again found that Haar over performs to CDF9/7. Next, the study is carried on high capacity and secure steganography scheme MLSB-VM for grayscale images and finally a modified Fusion scheme for color images is proposed. A comparative study of image steganography based on its different characteristics is provided for each of the schemes. The experimental results of proposed algorithm based on LSB varying mode method (Algo 4.4.1) have shown the high embedding rate, acceptable imperceptibility and better run time than the known DWT based algorithm. The proposed algorithm (Algo 4.5.1) based on Fusion method provides multi-level security and maximum embedding capacity in the cover image (3 times the number of pixels contained in the cover). The Algo 4.5.1 is further found to be robust against noise such as Gaussian and Salt-n-Pepper noise.

In Chapter 5, a data hiding is done using Discrete Slantlet Transform. According to Selesnick (1998-99), Slantlet transforms (SLTs) show a good trade-off between the time-localization and the smoothness properties of a signal. It is found experimentally that the Slantlet based MLSB-FM technique gives better PSNR values than the CDF9/7 based MLSB-FM technique. Structural similarity of images is found to be independent of image formats and provable security is found to be satisfactory except for the tested .tif images. The reason of this could be the intrinsic propertied of images or that .tif images are not good tolerant of quantization. In the case of high payload MLSB_VM method, it is observed that run time complexity of MLSB-VM method improves using the Slantlet transform in place of Haar wavelet. On comparing the performance of MLSB-VM method based on SLT in terms of PSNR, MSSIM (with same capacity) and KLDiv with the corresponding HWT/CDF9/7 methods it is observed that SLT based MLSB-VM is performing better than CDF9/7 whereas results of PSNR, SSIM and KLDiv for HWT based MLSB-VM obtained of different image formats is found to be
better. Fusion method for color images based on SLT has shown to be the best scheme that provides high stego-image at quality and high payload. Though, the method does show good provable security in terms of KLDiv as well as structural similarity in terms of SSIM, but it is not found to be robust to statistical attacks.

In Chapter 6, Irreversible Image Steganography using the Contourlet Transform (CTT) for the grayscale and color images has been presented. Contourlet transform has the advantages of high capacity than the DWT and SLT (that have 3 middle and high frequency sub-bands in level 2 whereas in 2-level CTT, we obtain 4 directional sub-bands). In the MLSB-FB and MLSB-VM techniques based on CTT, experimental results show better imperceptibility (PSNR) than the CDF9/76 and SLT based MLSB methods. However, Haar based MLSB techniques still show best PSNR than CTT. The results of KLDiv for CTT based MLSB-FM shows improvement over the SLT based MLSB-FM for all the image formats whereas it shows improvement against Haar based MLSB-FM for the new11.tif and new12.tif. Similar results are obtained for Structural Similarity for all the images except for new11.tif. In the MLSB-VM approach, CTT performs better in terms of structural similarity and provable security than SLT and CDF9/7 irrespective of image format. Through the histogram analysis it is found that MLSB-FM based on CTT does not resist statistical attacks. In the MLSB-VM scheme using CTT, it is observed that the image formats .bmp, .jpg and .png can resist the statistical attacks. However, MLSB-VM using CTT scheme is found to be poor against statistical attacks for the tested .tif format images. Fusion method based CTT does show high image quality, better SSIM and KLDiv than SLT based method, but it only shows the resistance against statistical attacks for .png image formats.

In Chapter 7, the applications of complex wavelets introduced by Selesnick (2001, 2004), DD DWT and DD DT DWT to image steganography are investigated and comparison study of the proposed steganographic schemes based on them is given with the other transforms such as DWT, SLT and CTT. It is found through experimental results based on MLSB-FM and MLSB-VM schemes for grayscale images that DD DWT domain is a better option than others for image steganography as it offers much better imperceptibility, structural similarity and provable security. Further, these schemes are high rate of embedding schemes. The resistance to statistical attacks is
shown by the MLSB-FM/MLSB-VM based DD DWT scheme to some extent. Though, MLSB-FM method based on DD DT DWT fails against Gaussian noise attack. Forward Real DD DT DWT shows better option for the Fusion method in color images in achieving good imperceptibility, structural similarity and provable security than other transforms. Further, the results of KLDiv are found to be independent of image formats. Histogram analysis is found to be in favor of DD DWT or DD DT DWT as distortions in the histograms of stego-images are obvious.

In Chapter 8, Chapter 9 and Chapter 10, Two types of reversible Companding technique are presented using DWT, SLT, CTT, DD DWT and DD DT DWT called as Perceptual Reversible Data Hiding (P-RDH) and Robust Reversible Data Hiding (R-RDH). In Chapter 8, we first discuss the P-RDH using Companding technique in the Wavelets and SLT domain and present the comparative analysis between them. We also present the R-RDH based on SLT. HWT based Companding technique is compared with CDF9/7 wavelet based Companding technique in Section 8.2. The Haar wavelet has shown better performance in terms of imperceptibility, structural similarity and provable security. On the other hand, CDF9/7 is found to be better in the recovery of original image (Figure 8.2.5). Next, P-RDH based on SLT is presented and is compared with the corresponding DWT based algorithm. It is observed that the SLT provides better imperceptibility than Haar for tested images of .jpg, .png and .bmp formats. Structural similarity of images is shown to be better than CDF9/7 and close to the results of Haar based P-RDH which are ≈ 1. The R-RDH based on SLT is discussed next which make use of AES technique to encrypt the encoded message at the pre-processing level of algorithm. AES algorithm is a very secure technique for cryptography and the techniques which use frequency domain are considered highly secured for system for the combination of steganography. The integration of Compression technique (T-codes) and cryptography technique (Modified AES) with Steganography use three keys – encoding key, encrypted key and threshold value, making the present algorithm more secure. The proposed R-RDH method provides not only acceptable image quality but also has almost no distortion in the stego-image after adding Gaussian noise or Salt and Pepper noise. The P-RDH algorithm based on SLT is extended to CTT in Chapter 9. The experimental results show that CTT based RDH is
better than CDF9/7 and SLT in terms of imperceptibility, structural similarity and provable security. As compare to Haar, CTT shows better results in terms of PSNR when normalization process is used. Haar based RDH still shows better results of SSIM and KLDiv on average than CTT based RDH. In Chapter 10, both the reversible techniques, perceptual and robust, have been covered using complex wavelet transforms such as DD DWT and DD DT DWT. The use of DD DT DWT for reversible steganography method has shown improvements over the other transforms, DWT, SLT and CTT in terms imperceptibility (PSNR), structural similarity (SSIM), provable security (KLDiv) and embedding capacity. The approach presented in the Chapter 7 and next in Chapter 10 using Complex Wavelet Transforms, DD DWT and Forward Real DD DT DWT (Selesnick) in image steganography opens the door for developing more noval data hiding techniques and exploring/using other redundant and nonredundant complex wavelet transforms as tool in information hiding.

The conclusions and the future work is given in Chapter 11.